Приложение 3 к приказу №149

# ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОГБУЗ «ИГП № 11»

г. Иркутск,
2017

# ОГЛАВЛЕНИЕ

# I. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением об обработке и защите персональных данных Работников (далее – Положение) устанавливается порядок обработки персональных данных Работников ОГБУЗ «ИГП № 11» (далее Поликлиника или Работодатель) и гарантии конфиденциальности сведений, предоставляемых Работником Работодателю.

1.2. Работниками являются физические лица (субъекты персональных данных), заключившие с Работодателем трудовые договоры.

1.3. Обработка персональных данных Работников в Поликлинике заключается в сборе, записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), извлечении, использовании, передаче (распространении, предоставлении, доступе), обезличивании, блокировании, удалении, уничтожении и в защите от несанкционированного доступа к персональным данным.

1.4. Настоящее Положение и изменения к нему утверждаются Главным врачом Поликлиники и вводятся в действие приказом по основной деятельности Поликлиники. Все Работники Поликлиники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение является обязательным для исполнения всеми Работниками Поликлиники, имеющими доступ к персональным данным Работников.

## 2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под персональными данными Работников понимается информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника, а также сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющие идентифицировать его личность.

2.2. Персональные данные Работника, обработка которых осуществляется в Поликлинике, включают следующие документы и сведения:

- фамилия, имя, отчество;
- фамилия при рождении (либо другие фамилии, если они были);
- день, месяц, год и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и

местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

- копии документов об образовании;
- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и иные сведения;
- копии документов о повышении квалификации;
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона работодателя, а также реквизитов иных организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также иные сведения;
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и дата изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- вторые экземпляры трудового договора с Работниками;
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- трудовые книжки и вкладыши к ним;
- карточки унифицированной формы Т-2 «Личная карточка работника»;
- личные дела Работников в бумажной форме;
- фотографическое изображение работника;
- сведения о заработной плате (номера счетов для расчета с Работниками, в том числе номера их банковских карточек);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и иные сведения;
- копии военных билетов;
- сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и) или иных членов семьи, паспортные данные супруга(и) или иных членов семьи (паспортные данные или данные свидетельства о рождении), данные справки по форме 2НДФЛ супруга(и) или иных членов семьи;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;

- сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);
- сведения, указанные в оригиналах и копиях приказов по персоналу Поликлиники и материалах к ним, в том числе информация об отпусках, о командировках и т.п.;
- оригиналы приказов, изданных в Поликлинике, и относящиеся к субъекту персональных данных, и материалы к данным приказам;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Поликлиники;
- материалы по аттестации и оценке Работников Поликлиники;
- материалы по внутренним служебным расследованиям в отношении Работников Поликлиники;
- сведения о временной нетрудоспособности Работников Поликлиники;
- табельный номер Работника Поликлиники;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и иные сведения);
- иные сведения, с которыми Работник считает нужным ознакомить Работодателя.

## 3. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Документы, перечисленные в п.2.2. Положения, содержащие сведения о персональных данных Работников Поликлиники, являются конфиденциальными. Поликлиника обеспечивает конфиденциальность персональных данных, и обязан не допускать их распространения без согласия Работника, либо наличия иного законного основания.

3.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Работников распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

## 4. ПРАВА И ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

4.1. Работодатель имеет право без согласия Работника осуществлять обработку его персональных данных в следующих случаях:

4.1.1. если обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации и в целях исполнения трудового договора с Работником;

4.1.2. если обработка персональных данных Работника осуществляется для статистических или иных научных целей при условии обязательного обезличивания его персональных данных;

4.1.3. если обработка персональных данных Работника необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно.

4.1.4. в случаях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

4.1.5. В иных случаях (не поименованных в п.4.1. Положения) Работодатель может осуществлять обработку персональных данных Работника только с письменного согласия Работника. Согласие на обработку персональных данных по основаниям данного пункта может быть отозвано Работником. Обязанность предоставить доказательство получения согласия Работника на обработку его персональных данных по основаниям данного пункта, возлагается на Работодателя.

4.2. Письменное согласие Работника на обработку своих персональных данных по основаниям пп.4.1.1. Положения должно включать в себя:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Работодателя, получающего согласие Работника;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие Работник;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- личную подпись Работника.

4.3. В целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных Работника обязаны соблюдать следующие общие требования:

- Обработка персональных данных Работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работникам в трудоустройстве, обучения и продвижении в Поликлинике, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- При определении объема и содержания персональных данных Работника, подлежащих обработке, Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами.

4.4. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.

4.5. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его членстве в организациях или его профсоюзной деятельности, за исключением случаев, предусмотренных действующим законодательством.

4.6. Работодатель не должен запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.

4.7. При принятии решений, затрагивающих интересы Работника, Работодатель не имеет права основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки.

4.8. Защита персональных данных Работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет средств Поликлиники в порядке, установленном федеральным законодательством.

## 5. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

5.1. Работник обязан передавать Работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации, настоящим Положением и Правилами внутреннего трудового распорядка, принятыми в Поликлинике.

5.2. Работник должен своевременно в срок, не превышающий пяти рабочих дней, сообщать Работодателю об изменении своих персональных данных.

5.3. В целях обеспечения защиты персональных данных, хранящихся у Работодателя, Работник имеет право:

5.3.1. На полную информацию о своих персональных данных и обработке этих данных; на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных федеральным законом.

Сведения о наличии персональных данных должны быть предоставлены Работнику в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.3.2. Определить своих представителей для защиты своих персональных данных.

5.3.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона.

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

5.5. При отказе Работодателя исключить или исправить персональные данные Работника последний имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия;

Персональные данные оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.6. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.7. Обжаловать в суде любые неправомерные действия или бездействие Работодателя при обработке и защите его персональных данных.

5.8. Передача информации третьей стороне возможна только при письменном согласии Работника, за исключением обстоятельств, установленных законодательством.

5.9. Если Работник считает, что Работодатель осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, Работник вправе обжаловать действия или бездействие Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5.10. Работник имеет право на сохранение и защиту своей личной и семейной тайны, на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.11. Во всех случаях отказ Работника от своих прав на сохранение и защиту конфиденциальности его персональных данных недействителен и юридически ничтожен.

## 6. СБОР И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Сбор персональных данных

– все персональные данные Работника Работодатель получает у него самого;

– если персональные данные Работника возможно получить только у третьей стороны, то Работник уведомляется об этом Работодателем заранее. Работодателем в этом случае должно быть получено письменное согласие Работника. Работодатель должен сообщить Работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и о последствиях отказа Работника дать письменное согласие на их получение;

– работник Поликлиники предоставляет работнику управления кадров достоверные сведения о себе. Информация, представляемая Работником при поступлении на работу в Поликлиника, должна иметь документальную форму. Работник управления кадров Поликлиники проверяет достоверность сведений, сверяя данные, предоставленные Работником, с имеющимися у Работника документами.

6.2. При заключении трудового договора в соответствии со ст.65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет Работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или Работник поступает на работу на условиях совместительства, либо трудовая книжка у Работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника);
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям.

6.3. Документы, содержащие персональные данные Работника, создаются путём:

- создания комплекта документов, сопровождающих процесс оформления трудовых отношений Работника в Поликлинике при его приеме, переводе и увольнении методом внесения сведений в учётные формы (на бумажных и электронных носителях);
- копирования оригиналов документов (документ об образовании, свидетельство ИНН, пенсионное свидетельство);
- получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография).

6.4. При поступлении на работу в Поликлиника:

- Работником управления кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные Работника:
  – общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные, сведения о месте жительства и контактных телефонах);
  – сведения о воинском учете;
  – данные о приеме на работу;

  В дальнейшем в личную карточку вносятся:

  – сведения о переводах на другую работу;
  – сведения об аттестации;
  – сведения о повышении квалификации;
  – сведения о профессиональной переподготовке;
  – сведения о наградах (поощрениях), почетных званиях;
  – сведения об отпусках;
  – сведения о социальных гарантиях;
  – сведения об изменении места жительства, контактных телефонов.

6.5. Личное дело Работника оформляется после издания приказа о приеме на работу.

- Все документы личного дела подшиваются в обложку образца, установленного в Поликлинике. На ней указываются фамилия, имя отчество Работника, номер личного дела. К каждому личному делу прилагается фотография Работника размером 3х4.

- Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитые в личное дело, нумеруются.

- Личное дело ведется на протяжении всей трудовой деятельности Работника в Поликлинике. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

6.6. Хранение персональных данных

6.6.1. Персональные данные Работников могут храниться, как на бумажных носителях, так и в электронном виде.

6.6.2. В отделе кадров Поликлиники хранятся в специально отведенных системах хранения (шкафах, сейфах) согласно приказу, определяющему места хранения носителей персональных данных следующие группы документов, содержащие данные Работников в единичном или сводном виде:

- документы, содержащие персональные данные Работников (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекты документов по тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Поликлиники, руководителям структурных подразделений; копии отчетов, направляемых в государственные

органы статистики, налоговые инспекции, вышестоящие органы управления и другие ведомства.

- документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции Работников, приказы, распоряжения, указания руководства Поликлиники); документы по планированию, учету, анализу и отчетности в части работы с персоналом Поликлиники.

6.6.3. В том числе в специально отведенных системах хранения (шкафах, сейфах) согласно приказу, определяющему места хранения носителей персональных данных, хранятся:

- трудовые книжки, личные карточки Работников по форме Т-2;
- личные дела в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела находятся в отделе кадров.

6.6.4. Ключи от шкафов, сейфов хранятся у начальника отдела кадров лично.

6.7. Персональные данные Работников могут также храниться в электронном виде в информационных системах персональных данных Поликлиники, в электронных папках и файлах в ПК работников Поликлиники.

Доступ к ПК строго ограничен кругом лиц, определённых приказом Главного врача Поликлиники.

6.8. Хранение персональных данных в бухгалтерии:

- согласно приказу, определяющему места хранения носителей персональных данных, персональные данные, содержащиеся на бумажных носителях, хранятся в шкафах, сейфах согласно приказу, определяющему места хранения носителей персональных данных, установленных в служебных помещениях, занимаемых главным бухгалтером и иными работниками бухгалтерии.
- персональные данные, содержащиеся на электронных носителях информации, хранятся согласно приказу, определяющему места хранения носителей персональных данных.

6.10. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

6.11. Персональные данные, содержащиеся на электронных носителях информации, уничтожаются по акту по истечению установленного срока хранения.

## 7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При передаче персональных данных Работника Работодатель должен соблюдать следующие требования:

- не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных федеральным законом;

- предупредить лиц, получающих персональные данные Работника о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- разрешать доступ к персональным данным Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Работника, которые необходимы для выполнения конкретных функций;

- передавать персональные данные Работника представителям Работников в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными Работника, которые необходимы для выполнения указанными представителями их функций.

7.2. Передача персональных данных Работника третьим лицам осуществляется только с письменного согласия Работника, которое оформляется по установленной форме (Приложение №1) и должно включать в себя:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Работодателя, получающего согласие Работника;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие Работник;
- срок, в течение которого действует согласие, а также порядок его отзыва.

- Согласия Работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника; когда третьи лица оказывают услуги Работодателю на основании заключенных договоров, а также в случаях, установленных действующим законодательством и настоящим Положением.

- Работники Работодателя, передающие персональные данные Работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме (Приложение №3), и должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

7.2. Передача документов (иных материальных носителей), содержащих персональные данные Работников, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Поликлинике;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных Работника;

- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные Работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных Работника Поликлиники несет начальник отдела кадров, а также работник, осуществляющий передачу персональных данных Работника третьим лицам.

7.3. Представителю Работника персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя Работника;

- письменного заявления Работника, написанного в присутствии работника управления кадров Работодателя (если заявление написано Работником не в присутствии работника управления кадров, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе кадров в личном деле Работника.

7.4. Предоставление персональных данных Работника государственным органам производится в соответствии с требованиями действующего законодательства.

7.5. Персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника, за исключением случаев, когда передача персональных данных Работника без его согласия допускается действующим законодательством Российской Федерации.

7.6. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии письменного согласия Работника, удостоверенного нотариально.

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

## 8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

8.1. Право доступа к персональным данным Работника в Поликлинике имеют:

- Главный врач;

- начальник и работники управления кадров;

- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);

- при переводе из одного структурного подразделения в другое, доступ к персональным данным Работника может иметь руководитель нового подразделения;

- сам Работник – субъект персональных данных;

- другие работники Поликлиники при выполнении ими своих служебных обязанностей.

8.2. Перечень работников Поликлиники, имеющих доступ к персональным данным Работников, определяется приказом Главного врача Поликлиники.

## 9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

9.1. Поликлиника обязана при обработке персональных данных принимать необходимые организационные и технические меры для защиты персональных данных Работников от

неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

9.2. Защите подлежит:

- информация о персональных данных Работника, содержащаяся на бумажных носителях;
- документы, содержащие персональные данные Работника;
- персональные данные, содержащиеся на электронных носителях.

9.3. Общую организацию защиты персональных данных Работников по указанию Главного врача осуществляет назначенный работник, ответственный за организацию обработки персональных данных, и начальник отдела кадров в соответствии с должностными инструкциями.

9.4. Начальник отдела кадров обеспечивает:

- Ознакомление работника под роспись с настоящим Положением.

- Истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки.

- Ознакомление работника под роспись с приказами и иными внутренними локальными нормативными актами, регулирующими обработку и защиту персональных данных в Поликлинике.

- Общий контроль соблюдения Работниками мер по защите персональных данных.

9.5. Защита информационных систем Поликлиники, в которых обрабатываются персональные данные Работников, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке, осуществляется в соответствии с Положением о мерах по организации защиты информационных систем персональных данных Поликлиники.

9.6. Доступ к персональным данным Работника имеют работники Работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией Главного врача, доступ к персональным данным Работника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей работников, имеющих доступ к персональным данным Работника Поликлиники, и которым они необходимы в связи с исполнением трудовых обязанностей.

9.6.1. Все работники, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных Работников (соглашение о неразглашении конфиденциальной информации).

Процедура оформления доступа к персональным данным Работника включает в себя:

- ознакомление Работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных Работника, с данными актами также производится ознакомление Работника под подпись.

- истребование с работника (за исключением Главного врача) письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки, подготовленного по установленной форме.

9.6.2. Работник Работодателя, имеющий доступ к персональным данным Работников в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные Работника, исключающее доступ к ним третьих лиц.

В отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные Работников.

- При уходе в отпуск, во время служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Работников лицу, на которое локальным актом Поликлиники (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения.

9.6.3. При увольнении работника, имеющего доступ к персональным данным Работников, документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения или Главному врачу.

9.6.4. Допуск к персональным данным Работника других работников Работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

9.7. Личные дела и документы, содержащие персональные данные Работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

9.7.1. В Поликлинике не допускается выдача личных дел работников на рабочие места руководителей структурных подразделений. Личные дела могут выдаваться только Главному врачу. В исключительных случаях, по письменному разрешению Главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации Работника).

9.7.2. В конце рабочего дня все личные дела, выданные работникам, имеющим право доступа к этим документам, сдаются в управление кадров.

9.8. Защита доступа к электронным носителям, содержащим персональные данные Работников, обеспечивается, том числе:

- использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный доступ к персональным данным;
- разграничением прав доступа с использованием учетной записи;
- 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;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- контролем эффективности принимаемых мер по обеспечению защищенности персональных данных.

9.9. Копировать и делать выписки персональных данных Работника разрешается исключительно в служебных целях с письменного разрешения начальника управления кадров.

9.10. Ответы на письменные запросы других организаций и учреждений о персональных данных Работников Поликлиники даются только с письменного согласия самого Работника, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Поликлиники, и в том объеме, который позволяет не разглашать излишний объем персональных сведений о Работниках Поликлиники.

9.11. Передача информации, содержащей сведения о персональных данных Работников Поликлиники, по телефону, факсимильной связи, электронной почте запрещается.

## 10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

10.1. Главный врач, разрешающий доступ работника к документам, содержащим персональные данные Работника, несет персональную ответственность за данное разрешение.

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

10.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

10.4. За неисполнение или ненадлежащее исполнение Работником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных Работников Работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

10.4.1. К лицам, виновным в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, могут быть применены следующие дисциплинарные взыскания:

а) замечание;
б) выговор;
в) увольнение.

10.4.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

10.4.3. Приказ о применении к Работнику дисциплинарного взыскания с указанием оснований его применения объявляется Работнику под роспись в течение трех рабочих дней со дня его издания, не считая времени отсутствия работника на работе.

10.4.4. Если в течение года со дня применения дисциплинарного взыскания Работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с Работника по собственной инициативе, по письменному заявлению Работника или по ходатайству его непосредственного руководителя.

10.5. Должностные лица, в обязанность которых входит ведение персональных данных работника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной

информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

10.6. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на Работников.

10.7. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

## 11. СПИСОК ИСПОЛЬЗОВАННЫХ ЗАКОНОДАТЕЛЬНЫХ И НОРМАТИВНЫХ АКТОВ

Разработка настоящего Положения осуществлена в соответствии со следующими нормативными документами:

Конституция Российской Федерации (часть 1 статьи 23, статья 24);

Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ;

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

# II. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНТРАГЕНТОВ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением об обработке и защите персональных данных контрагентов (далее – Положение) устанавливается порядок обработки персональных данных контрагентов ОГБУЗ «ИГП № 11» (далее – Поликлиника или Оператор) и гарантии конфиденциальности сведений, предоставляемых контрагентами Поликлинике.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иными нормативными актами, действующими на территории Российской Федерации.

1.3. Действие настоящего Положения распространяется на всех работников Поликлиники и доводится до сведения работников под подпись.

1.4. Настоящее Положение вступает в силу со дня его утверждения Руководителем Поликлиники. Все изменения в настоящее положение вносятся приказом Руководителя Поликлиники.

1.5. В настоящем Положении используются следующие термины и определения:

- Оператор – Поликлиника. Осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными контрагентов.
- Контрагент – физическое лицо, официальный представитель – физическое лицо юридического лица и/или индивидуального предпринимателя, вступившее в договорные отношения с Поликлиникой.
- Персональные данные Контрагента – персональные данные, необходимые Оператору в связи с исполнением договорных отношений и касающаяся конкретного Контрагента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия (должность), номер контактного телефона, адрес электронной почты.
- 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.
- Защита персональных данных Контрагента – деятельность Поликлиники по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер обеспечения конфиденциальности информации.
- Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения и передачи третьим лицам без согласия субъекта персональных данных или наличия иного законного основания.

## 2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные Контрагента относятся к категории конфиденциальной информации.

2.2. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных Контрагента соблюдают следующие общие требования:

- обработка персональных данных Контрагента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации.
- все персональные данные Контрагента Оператор получает у него самого, за исключением случаев, когда их получение возможно только у третьей стороны способом, не противоречащим законодательству Российской Федерации.
- обработка персональных данных, полученных от третьих лиц, возможна только при уведомлении субъекта персональных данных об этом заранее.

2.3. Оператор не получает и не обрабатывает персональные данные Контрагента о его политических, религиозных и иных убеждениях и частной жизни.

2.4. Персональные данные не используются в целях причинения имущественного и морального вреда Контрагенту, затруднения реализации его прав и свобод.

2.5. При принятии решений, затрагивающих интересы Контрагента, Оператор не основывается на персональных данных Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

2.6. При идентификации Контрагента Оператор требует предъявление документов, удостоверяющих личность и подтверждающих полномочия представителя.

2.7. При заключении договора, как и в ходе его исполнения, в случае возникновения необходимости, Заказчик может потребовать предоставление Контрагентом иных документов, содержащих информацию о нем, с момента предоставления которых может быть связано предоставление дополнительных гарантий и компенсаций.

2.8. После принятия решения о заключении договора или предоставления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, персональные данные Контрагента, также будут включены в:

- договоры;
- иные документы, включение в которые персональных данных Контрагента необходимо согласно действующему законодательству Российской Федерации (накладные, акты, отчеты и т.д.).

## 3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Все работники, имеющие доступ к персональным данным Контрагентов, подписывают «Соглашение о неразглашении конфиденциальной информации».

3.2. Защита персональных данных Контрагентов от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством Российской Федерации, внутренними регламентирующими документами Поликлиники.

3.3. Защите подлежат:

- персональные данные, содержащиеся на электронных и материальных носителях;
- носители, содержащие персональные данные.

3.4. Ответственные лица структурных подразделений Поликлиники, хранящих персональные данные на бумажных и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования.

3.5. Ответственные лица, обрабатывающие персональные данные в информационных системах персональных данных и на машинных носителях информации, обеспечивают защиту в соответствии с требованиями законодательства Российской Федерации, нормативными и методическими документами, касающимися защиты персональных данных.

## 4. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сведения о Контрагентах на бумажных носителях хранятся в помещениях Поликлиники. Для хранения носителей используются шкафы (ящики), расположенные внутри контролируемой зоны Поликлиники.

4.2. Обязанности по хранению документов, в которых содержатся персональные данные Контрагентов, возлагаются на руководителей структурных подразделений, в которых обрабатывается информация.

4.3. Ключи от шкафов /ящиков (при наличии), в которых хранятся носители ПДн, находятся у работника, обрабатывающего данную информацию.

4.4. Персональные данные Контрагентов могут также храниться в электронном виде – на электронных носителях информации, доступ к которым ограничен и регламентируется Поликлиникой.

4.5. Доступ к персональным данным Контрагентов без специального разрешения имеют работники, занимающие в Поликлинике следующие должности:

- Главный бухгалтер
- Главный врач
- Заместитель главного бухгалтера
- Заместитель главного врача по оранизационно-методической работе
- Заместитель главного врача по финансово-экономической работе – начальник планово-экономического отдела
- Кассир
- Оператор
- Программист
- Экономист
- Юрисконсульт

К обработке персональных данных Контрагентов допускаются работники Поликлиники в соответствии с Приказом «Об утверждении перечней должностей и лиц, допущенных к обработке персональных данных».

4.6. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено законодательством Российской Федерации, вышеуказанные персональные данные уничтожаются.

## 5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче персональных данных Контрагента Оператор соблюдает следующие требования, и выполняются следующие условия:

- осуществляет обработку персональных данных Контрагента в пределах своей организации в соответствии с настоящим Положением;

- разрешает доступ к персональным данным Контрагентов только специально уполномоченным лицам, при этом указанные лица вправе получать только те персональные данные Контрагента, которые необходимы для выполнения конкретных функций;
- вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством;
- определяет требования к защите обрабатываемых персональных данных и перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, а так же устанавливает обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- в случае если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором;
- передает персональные данные Контрагента его представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными Контрагента, которые необходимы для выполнения указанными представителями их функций.

5.2. В случае если Оператору оказываются услуги, выполняются работы или осуществляется поставка товаров юридическими или физическими лицами на основании заключенных договоров (либо иных оснований), и в силу данных договоров эти лица должны иметь доступ к персональным данным, то необходимые персональные данные предоставляются Оператором при наличии в заключенном договоре условия о неразглашении конфиденциальной информации (в том числе содержащей персональные данные или составляющую коммерческую тайну) либо после подписания с указанными лицами Соглашения о неразглашении информации, содержащей персональные данные (неразглашении конфиденциальной информации).

5.3. Все сведения о передаче персональных данных Контрагентов регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

## 6. ОБЯЗАННОСТИ КОНТРАГЕНТА И ОПЕРАТОРА

6.1. В целях обеспечения достоверности персональных данных, Контрагент обязан:

- при заключении договора предоставить Оператору полные и достоверные данные о себе;
- в случае изменения сведений, составляющих персональные данные Контрагента, не позднее пяти рабочих дней, предоставить обновленную информацию Оператору.

6.2. Оператор обязан:

- обеспечить защиту персональных данных от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;
- ознакомить субъекта персональных данных с действующими внутренними правилами обработки персональных данных;
- обеспечить защищенное хранение документов, содержащих персональные данные. При этом персональные данные не должны храниться дольше, чем этого требуют цели, для которых они были получены, или дольше, чем это требуется в интересах лиц, о которых собраны данные, или дольше, чем этого требует законодательство;

- вести учет передачи персональных данных Контрагентов третьим лицам путем ведения соответствующего Журнала учета передачи персональных данных;
- в случае реорганизации или ликвидации Оператора, учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации;
- вести Журнал учета обращений субъектов персональных данных;
- осуществлять передачу персональных данных субъекта только в соответствии с законодательством Российской Федерации и настоящим Положением;
- по требованию субъекта персональных данных или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

## 7. ПРАВА КОНТРАГЕНТОВ В ЦЕЛЯХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Контрагенты имеют право на:

- получение полной информации о составе своих персональных данных и их обработке, в частности, Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных;
- бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Контрагента на основании письменного запроса, за исключением случаев, если предоставление персональных данных нарушает конституционные права и свободы других лиц;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные Контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия;
- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суде или надзорном органе любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

## 8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ПОЛУЧЕНИЕ, ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

# III. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Согласно ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную, семейную тайну, защиту своей чести и доброго имени, реализация которого обеспечивается положением ст. 24 Конституции РФ, устанавливающим, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. В соответствии с законодательством Российской Федерации информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных действующим законодательством. Отношения, связанные с обработкой персональных данных, осуществляемой юридическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, регулируются Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

Настоящее Положение разработано в целях выполнения указанных выше норм Конституции РФ, в соответствии с требованиями законодательства Российской Федерации и иных нормативных правовых актов в сфере охраны здоровья населения и обработки персональных данных.

1.2. Настоящее Положение определяет порядок работы (получения, обработки, использования, передачи, хранения и т.д.) сотрудников медицинской организации (далее Оператор) с персональными данными пациентов и гарантии конфиденциальности сведений о пациенте, предоставленных пациентом в медицинской организации; права пациента при обработке его персональных данных; ответственность лиц за невыполнение требований норм, регулирующих обработку персональных данных пациента.

## 2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА

2.1. Персональные данные пациента - любая информация, относящаяся к прямо или косвенно к пациенту (субъекту персональных данных).

.

2.2. В целях ведения персонифицированного учета осуществляется обработка следующих персональных данных о лицах, которым оказываются медицинские услуги (пациентах):

- фамилия;
- имя;
- отчество;
- пол;
- дата рождения;
- реквизиты документа удостоверяющего личность;
- адрес места жительства;
- адрес места регистрации;
- контактные телефоны;
- место работы;

- национальность;
- реквизиты полиса обязательного (добровольного) медицинского страхования застрахованного лица;
- страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
- данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью и другую информацию - в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг по договору.

Все персональные данные, касающиеся состояния здоровья пациента, относятся к специальным категориям персональных данных и обрабатываются в соответствии с установленным законодательством и иными нормативными правовыми актами требованиями.

## 3. СБОР, ЦЕЛИ ОБРАБОТКИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА

3.1. Обработка персональных данных осуществляется:

- после получения письменного согласия субъекта персональных данных, составленного по утверждённой Оператором форме, соответствующей требованиям федерального закона, за исключением случаев, предусмотренных частью 2 статьи 6 ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в орган государственного надзора в сфере связи, информационных технологий и массовых коммуникаций территории, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных»;

- после принятия Оператором необходимых мер по защите персональных данных.

3.2. Все персональные данные пациента следует получать лично у пациента или у его законного 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.

3.3. Оператор сообщает пациенту или его законному представителю о целях обработки персональных данных, предполагаемых источниках и способах получения персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

3.4. Оператор осуществляет обработку персональных данных только после получения письменного согласия пациента (или его законного представителя) на обработку его персональных данных за исключением случаев, предусмотренных действующим законодательством.

3.5. При обращении за медицинской помощью пациент (или его законный представитель) предоставляет Оператору персональные данные о себе в документированной форме. А именно:

- паспорт или иной документ, удостоверяющий личность;
- полис обязательного медицинского страхования;
- направление (при наличии).

При отсутствии документов пациент (или его законный представитель) предоставляют Оператору необходимые персональные данные в устной форме.

3.6. Оператор с согласия пациента может запрашивать и получать персональные данные пациента, используя информационные системы персональных данных с применением средств автоматизации.

3.7. Обработка Оператором персональных данных пациента осуществляется исключительно в целях оказания пациенту качественной медицинской помощи в необходимых объёмах, соблюдения требований действующего законодательства, иных нормативных правовых актов, обеспечения контроля объёмов и качества оказанной медицинской помощи.

3.8. Оператор при определении объема и содержания обрабатываемых персональных данных пациента руководствуется Конституцией Российской Федерации, Основами законодательства Российской Федерации об охране здоровья граждан, иными нормативными правовыми актами в сфере охраны здоровья населения и обработки персональных данных.

3.9. Защита персональных данных пациента от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств в порядке, установленном законодательством, и принятыми Оператором в соответствии с ним локальными нормативными актами.

## 4. ПОРЯДОК ИСПОЛЬЗОВАНИЯ, ХРАНЕНИЯ, ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА

4.1. Персональные данные пациентов предоставляются Оператору после получения соответствующего информированного согласия пациентов на обработку их персональных данных. Персональные данные пациентов у Оператора содержаться в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. В информационных системах персональные данные могут быть размещены на материальных, в том числе бумажных носителях (медицинская карта пациента, иные медицинские документы).

4.2. Доступ к обработке персональных данных пациентов (как с использованием средств автоматизации, так и без использования средств автоматизации) обеспечивается в установленном Оператором порядке.

4.3. Конкретные обязанности по работе с информационными системами персональных данных и материальными носителями информации, в том числе с медицинскими документами, содержащими персональные данные пациентов возлагаются на сотрудников Оператора и закрепляются в должностных инструкциях.

4.4. Работа с информационными системами персональных данных, материальными носителями, в том числе с медицинской документацией, содержащими персональные данные пациентов осуществляется в специально отведённых для этого помещениях: ординаторские, кабинеты врачей, орг.-метод. отдел, кабинет медицинской статистики, регистратура, серверная и т.д.

4.5. Требования к месту обработки персональных данных, в том числе к серверной, обеспечивающие их защищённость устанавливаются Оператором.

4.6. Перечень лиц, имеющих право доступа к персональным данным пациентов и обработке их персональных данных, определяется приказом руководителя Оператора.

4.7. С лицами, допущенными к обработке персональных данных пациентов, заключается Соглашение о неразглашении.

4.8. Лица, допущенные в установленном порядке к обработке персональных данных, имеют право обрабатывать только те персональные данные пациентов, которые необходимы для выполнения
конкретных функций.

4.9. Оператор при создании и эксплуатации информационных систем персональных данных пациентов с использованием средств автоматизации обеспечивает проведение

классификации информационных систем (определение уровня защищенности) в установленном порядке.

4.10. Оператор при создании и эксплуатации информационных систем персональных данных пациентов с использованием средств автоматизации и без использования средств автоматизации принимает все необходимые организационные и технические меры, обеспечивающих выполнение установленных действующим законодательством требований к обработке персональных данных.

4.11. Оператор при осуществлении обработки персональных данных пациентов без использования средств автоматизации выполняет следующие требования.

4.11.1. При ведении журналов (реестров, книг, иных документов), содержащих персональные данные пациентов, необходимые для организации оказания медицинской помощи, Оператор соблюдает следующие условия:

- необходимость ведения такого журнала (реестра, книги, иных документов) предусматривается приказом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги, иных документов), сроки обработки персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах, иных документах) информации не допускается, за исключением случаев, предусмотренных действующим законодательством.

4.11.2. Обработка персональных данных пациентов, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных пациентов можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.11.3. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4.11.4. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

4.11.5. Уточнение персональных данных пациента 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.

4.12. С согласия пациента или его законного представителя допускается передача сведений, в том числе персональных данных, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.

4.13. Передача персональных данных пациента, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается может допускается в случаях, предусмотренных частью 4 статьи 13 Федерального закона Российской Федерации от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" (далее Основы):

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 Основ;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Основ, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Основ, для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Основами.

4.14. При передаче персональных данных пациента сотрудники медицинской организации должны соблюдать следующие требования:

- не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные пациента в коммерческих и иных целях без его письменного согласия;

- предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности);

- разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, определенным приказом Руководителя, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных должностных функций;

- передавать персональные данные пациента представителям пациента в порядке, установленном законодательством, и ограничивать эту информацию только теми персональными данными пациента, которые необходимы для выполнения указанными представителями их функций.

4.15. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

4.16. Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

## 5. ПРАВА ПАЦИЕНТОВ ПРИ ОБРАБОТКЕ ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

5.1. В целях обеспечения защиты своих интересов, реализации прав и свобод в сфере персональных данных, регламентированных действующим законодательством пациенты, их законные представители, а также представители имеют право на:

- предоставление Оператором полной информации об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные пациента, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование 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;
- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование действий или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Права пациента, представителя, законного представителя на доступ к своим персональным данным ограничиваются в случаях, предусмотренных действующим законодательством.

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

6.1 Лица, виновные в нарушении установленных требований в сфере обработки персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, законодательством, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

6.3. Сотрудники Оператора, получившие в установленном порядке доступ к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных обучающихся привлекаются к ответственности, предусмотренной действующим законодательством.

## 7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящее Положение вступает в законную силу с момента утверждения его руководителем Оператора и действует до утверждения нового положения.

# IV. ПОЛОЖЕНИЕ О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В Положении используются следующие понятия, определения и сокращения:

**ПДн** - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных.

**Обработка ПДн** - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

**ИСПДн** – информационная система персональных данных, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

**Автоматизированная обработка ПДн** – обработка ПДн с помощью средств вычислительной техники.

**Обработка ПДн без использования средств автоматизации** - обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Актуальные угрозы безопасности персональных данных** - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

**Система защиты персональных данных – СЗПДн** - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

**Закон «О персональных данных»** - Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

**Приказ ФСТЭК №21** - Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящее Положение о мерах по организации защиты информационных систем персональных данных в ОГБУЗ «ИГП № 11» (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности в ОГБУЗ «ИГП № 11» (далее – Поликлиника) на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются 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.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой Поликлиникой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 г.

№1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

2.2 Настоящее Положение является внутренним локальным актом Поликлиники.

Настоящее Положение вступает в силу с момента его утверждения Руководителем Поликлиники и действует бессрочно, до замены его новым Положением.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

Изменения к Положению утверждаются Руководителем Поликлиники.

2.3 Все работники Поликлиники должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

Настоящее Положение является обязательным для исполнения всеми работниками Поликлиники, имеющими доступ к ИСПДн.

2.4 Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Поликлинике уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных.

2.5 Положение разработано с учетом требований принятых в Поликлинике Политики по защите персональных данных в Поликлинике. Поликлиника учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Поликлиники, связанных с обработкой ПДн.

## 3. ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, в Поликлинике назначается уполномоченный сотрудник ответственный за обеспечение безопасности информационных систем персональных данных.

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

3.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется в соответствии с требованиями Приказа ФСТЭК № 21, а также иными нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

3.5. Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона «О персональных данных».

3.6. Поликлиника обеспечивает классификацию информационных систем в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы угроз актуальны для ИСПДн Поликлиники. По результатам определяется набор требований, которые необходимо выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации ИСПДн Поликлиники.

3.7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных и контроль за выполнением требований к защите ПДн при обработке их в ИСПДн организуется и проводится Поликлиникой самостоятельно, не реже 1 раза в 3 года в сроки, определяемые Поликлиникой.

## 4. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Состав и содержание организационных мер по обеспечению безопасности ПДн.

Необходимый уровень защищенности персональных данных при их обработке в информационных системах Поликлиники обеспечивается принятием следующих основных организационных мер:

1) введение режима обеспечения безопасности помещений, в которых размещены ИСПДн Поликлиники, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и обеспечивается Арендодателем;
2) обеспечение безусловной сохранности носителей персональных данных;
3) назначение уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных Поликлиники;
4) утверждение перечня персональных данных и иных объектов, подлежащих защите в ИСПДн Поликлиники;
5) утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн Поликлиники, необходим для выполнения ими служебных обязанностей;
6) проведение классификации ИСПДн Поликлиники, по результатам определяется набор требований, необходимых для обеспечения необходимого уровня защищенности ПДн;
7) обеспечение проведения не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и осуществление регулярного контроля за выполнением требований к защите ПДн при обработке их в ИСПДн.

4.2 Мероприятия по реализации организационных мер по обеспечению безопасности ПДн.

С учетом требований, перечисленных в пункте 1 статьи 6 Положения, проводятся следующие мероприятия:

1) Приказом Руководителя назначается уполномоченный сотрудник, ответственный за обеспечение безопасности информационных систем персональных данных Поликлиники. Разрабатывается и вводится в действие должностная инструкция, регламентирующая права и обязанности указанного сотрудника.
2) Вводится в действие приказ Руководителя «О создании Комиссии по персональным данным» (далее по тексту – Комиссия по персональным данным»).
3) Разрабатывается, утверждается и внедряется система организации доступа в помещения Поликлиники, где осуществляется обработка ПДн, исключающая возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности ИСПДн, хищения носителей информации ПДн.
4) Вводится в действие инструкция о порядке организации внутриобъектового и пропускного режимов в помещениях Поликлиники.

5) Определяются состав и категории обрабатываемых в Поликлинике персональных данных (результат оформляется в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Поликлинике).

6) Разрабатывается и вводится в действие инструкция пользователя ИСПДн, регламентирующая права и обязанности работника Поликлиники при работе с ИСПДн.

7) Разрабатывается и вводится в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в ИСПДн персональным данным.

8) Обеспечивается обучение Работников Поликлиники, осуществляющих обработку ПДн в информационных системах персональных данных, предусматривающее проведение не реже одного раза в год обучения пользованию средствами защиты информации, которые применяются в информационных системах Поликлиники, правилам работы с ними, правилам обработки ПДн, в соответствии с утвержденными в Поликлинике требованиями.

9) Разрабатывается и вводится в действие инструкция о порядке учета, использования, транспортировки, хранения и уничтожения в Поликлинике съемных носителей персональных данных.

10) Обеспечивается учет съемных носителей ПДн в каждом структурном подразделении Поликлиники (вводятся в действие журналы учета съемных носителей ПДн).

11) Локальными актами регламентирующими обработку и защиту персональных данных работников Поликлиники утверждаются перечни подразделений и работников, допущенных к обработке ПДн в информационных системах Поликлиники.

12) Принимается локальный нормативный акт об ответственности работников Поликлиники за разглашение персональных данных и несанкционированный доступ к персональным данным в информационных системах Поликлиники.

13) Комиссией по персональным данным проводятся внутренние проверки и классификация ИСПДн Поликлиники. Результаты оформляются в виде письменных отчетов, на основании которых разрабатывается план мероприятий по обеспечению безопасности ПДн в ИСПДн Поликлиники.

14) Разрабатывается и утверждается план внутренних проверок состояния защиты ПДн в Поликлинике. Вводится в действие журнал учета мероприятий по контролю соблюдения режима защиты персональных данных в информационных системах Поликлиники.

4.3 Технические меры по обеспечению безопасности ПДн в ИСПДн.

Поликлиника принимает технические меры по обеспечению безопасности информационных систем персональных данных.

План мероприятий по обеспечению защиты персональных данных в Поликлинике включает следующие этапы работы:

1) определение на основании Приказа ФСТЭК № 21 базового набора мер по обеспечению безопасности персональных данных в ИСПДн Поликлиники;

2) адаптация базового набора мер под ИСПДн Поликлиники с учетом особенностей их функционирования, исключая те меры, которые связаны с информационными технологиями, не используемыми в ИСПДн;

3) уточнение списка мер с включением в него не выбранных ранее мер для нейтрализации актуальных угроз;

4) внедрение дополнительных мер, обеспечивающих выполнение требований к защите персональных данных, установленных нормативными правовыми актами в

области обеспечения безопасности персональных данных и защиты информации.

В составе мер, входящих в план мероприятий по обеспечению защиты персональных данных в Поликлинике, в том числе, предусматривается:

1) внедрение системы парольной аутентификация работников Поликлиники, допущенных к работе с ИСПДн, предусматривающей определение минимальной длинны пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему и использование программных генераторов паролей;
2) установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в ИСПДн Поликлиники;
3) разработка и внедрение регламента обеспечивающего установку и запуск в ИСПДн только разрешенного к использованию в информационной системе программного обеспечения, и исключающего возможность использования запрещенного к использованию в информационной системе программного обеспечения;
4) разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
5) внедрение технологий, позволяющих осуществлять резервирование и восстановление работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
6) разработка инструкции, регламентирующей модификацию программного обеспечения и технических средств информационной системы персональных данных;
7) внедрение технологий, позволяющих осуществлять сбор, запись, хранение, анализ, просмотр и защиту информации о событиях безопасности в ИСПДн Поликлиники;
8) использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в ИСПДн вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования ПДн, иной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
9) проведение систематических мероприятий по анализу защищенности ИСПДн и тестированию работоспособности системы защиты персональных данных;
10) обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
11) разработка и ввод в действие электронного журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в ИСПДн.

## 5. ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общее руководство деятельностью Поликлиники по обеспечению безопасности ПДн осуществляет Руководитель.

5.2 Руководитель приказом назначает уполномоченного сотрудника, ответственного за обеспечение безопасности ИСПДн в Поликлинике.

5.3 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Поликлинике, получает указания непосредственно от Руководителя.

5.4 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Поликлинике, обязан не реже одного раза в три года проводить проверку состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.

5.5 Руководитель приказом создает в Поликлинике Комиссию по персональным данным, на которую возлагаются следующие обязанности:

1) реализация мероприятий, предусмотренных настоящим Положением;
2) осуществление внутреннего контроля и аудита соответствия практики обработки персональных данных в Поликлинике тем требованиям и нормам, которые установлены Законом «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Поликлиники;
3) организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.

5.6 Поликлиника на договорной основе имеет право привлечь для разработки и внедрения систем защиты ПДн в ИСПДн Поликлиники специализированные организации, имеющие лицензии ФСТЭК, ФСБ России на соответствующие виды деятельности.

## 6. ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн

6.1 Для ИСПДн, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:

1) изменение состава или структуры самой ИСПДн или технических особенностей ее построения (изменение состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
2) изменение состава угроз безопасности ПДн в ИСПДн;
3) изменение уровня защищенности, который необходимо обеспечить при защите ПДн.

6.2 Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится уполномоченным сотрудником, ответственным за обеспечение безопасности ИСПДн. Результаты проверки оформляются Отчетом по проведению внутренней проверки и утверждаются Руководителем.

## 7. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн

7.1 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн, и Комиссия по персональным данным периодически (не реже одного раза в год) должны проводить проверку соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

7.2 В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться разбирательство (внутренняя проверка).

7.3 В процессе проведения разбирательства необходимо провести разработку и

принятие мер по предотвращению возможных негативных последствий подобных нарушений.

7.4 По окончании проведения разбирательства готовится заключение о лицах, виновных в выявленных нарушениях.

# V. ПОЛОЖЕНИЕ О НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и устанавливает единый порядок неавтоматизированной обработки персональных данных в ОГБУЗ «ИГП № 11» (далее – Поликлиника).

1.2. В целях настоящего Положения используются следующие термины и понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных;
- обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3. Задачи, решаемые в процессе обработки персональных данных:

- документационное обеспечение обработки персональных данных;
- защита документированной информации, содержащей персональные данные.

## 2. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных статьей 6 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- после направления уведомления об обработке персональных данных в Поликлиника, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- после принятия необходимых мер по защите персональных данных.

2.2. В Поликлинике приказом Руководителя назначается работник, ответственный за организацию обработки и защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Работники, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением.

2.4. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.

## 3. СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

3.1. Система доступа представляет собой совокупность норм и правил, определяющих порядок предоставления работникам прав доступа документам, содержащим конфиденциальную информацию.

3.2. Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться работникам, письменно оформившим с Поликлиникой соглашение о неразглашении ставших им известными

конфиденциальных сведений. Письменное оформление соглашения о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа работников к документам;

- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного работника;

- система доступа должна давать возможность обеспечивать работников всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ к документам осуществляется согласно должностной инструкции.

3.3. Доступ работников Поликлиники к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом соблюдаются следующие условия:

- ознакомление работника под роспись с перечнем конфиденциальной информации;

- ознакомление работника под роспись с установленным в Поликлинике режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создание работнику необходимых условий для соблюдения им установленного режима по охране конфиденциальности.

3.4. Доступ работников Поликлиники к персональным данным осуществляется в соответствии с Перечнем допущенных к обработке персональных данных в Поликлинике.

3.5. Работник принимает следующие обязательства:

- по соблюдению установленного в Поликлинике режима по охране конфиденциальной информации;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в Соглашении о неразглашении конфиденциальной информации и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);

– о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации.

## 4. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

4.1. На бумажных носителях:

4.1.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных и магнитных носителях.

4.1.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.1.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

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

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

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

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Поликлиники, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

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

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

4.1.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

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

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

4.1.8. Правила, предусмотренные пунктами 4.1.6 и 4.1.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

4.2. В электронном виде без использования средств автоматизации:

4.2.1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.

4.2.2. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

4.2.3. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от иных зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

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

## 5. ПОДГОТОВКА И УЧЕТ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.2. Бланки типовых форм документов (справки, карточки, талоны, ведомости и т.п.) могут изготавливаться при помощи средств вычислительной техники или на компьютере.

5.3. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, рукописным способом.

5.4. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера.

## 6. ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ) ДОКУМЕНТОВ И ИХ УЧЕТ

6.1. Все документы, поступающие из иных организаций, подлежат регистрации в журнале учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления.

6.2. Пересылка документов может осуществляться через органы специальной связи или через почтовое отделение связи.

6.3. Об отправленных документах производятся соответствующие отметки в учетных формах.

### 7. КОПИРОВАНИЕ ДОКУМЕНТОВ

7.2. При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.

7.3. На некоторых документах может стоять отметка о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.

7.4. Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители структурных подразделений), наделенные правом распоряжения сведениями.

7.5. Разрешение на изготовление дополнительных экземпляров (копий) учтенного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.

### 8. РЕЖИМ СОХРАННОСТИ ДОКУМЕНТОВ

8.2. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.

8.3. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.

8.4. Право входа в такие помещения имеют руководитель организации и работники, имеющие прямое отношение к обработке и хранению документов.

## VI. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

При организации и проведении работ по обеспечению безопасности ПДн в Поликлинике, субъекты ПДн должны руководствоваться следующими нормативными и методическими документами:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»;
4. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
5. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
6. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Политика по защите персональных данных;

# VII. СПИСОК ПРИЛОЖЕНИЙ К ПОЛОЖЕНИЮ

Приложение №1. Согласие работника на обработку персональных данных;

Приложение №2. Согласие пациента на обработку персональных данных;

Приложение №3. Отзыв согласия на обработку персональных данных;

Приложение №4. Разъяснение субъекту персональных данных юридических последствий отказа от предоставления своих персональных данных;

Приложение №5. Соглашение о неразглашении конфиденциальной информации;

Приложение №6. Журнал учета передачи персональных данных;

Приложение №7. Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных;

Приложение №8. Акт приема-передачи документов (иных материальных носителей), содержащих персональные данные Работника.

Приложение №9. Типовая форма акта об уничтожении носителей, содержащих персональные данные;

Приложение №10. Журнал учета съемных носителей конфиденциальной информации (персональных данных).

**ПРИЛОЖЕНИЕ №1**
к Положению об обработке и защите персональных данных

# СОГЛАСИЕ
работника на обработку персональных данных

Я, _____
(Ф.И.О. работника)

зарегистрированный (ая) по адресу: _____

паспорт серия _____ № _____, выдан _____

_____ в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» даю согласие на обработку своих персональных данных ОГБУЗ «ИГП № 11» (Поликлиника) (далее - Оператор), расположенному по адресу: 664074 г. Иркутск ул. Лермонтова,89, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» со всеми данными, которые находятся в распоряжении Оператора.

1. Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя, отчество (в т.ч. предыдущие),
паспортные данные или данные документа, удостоверяющего личность,
дата рождения, место рождения,
гражданство,
отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке,
данные документов о подтверждении специальных знаний,
данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях,
знание иностранных языков,
семейное положение и данные о составе и членах семьи,
сведения о социальных льготах, пенсионном обеспечении и страховании,
данные документов об инвалидности (при наличии),
данные медицинского заключения (при необходимости),
стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
должность, квалификационный уровень,
сведения о заработной плате (доходах), банковских счетах, картах,
адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства,
номер телефона (стационарный домашний, мобильный),
данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (при наличии),
данные страхового свидетельства государственного пенсионного страхования,
данные страхового медицинского полиса обязательного страхования граждан,
личная фотография,
иные сведения, с которыми работник считает нужным ознакомить Оператора, либо дополнительная информация необходимая Оператору.

2. Цели обработки:
Вышеуказанные персональные данные предоставляю для обработки в целях соблюдения требований трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, продвижении по службе, обеспечения личной безопасности, контроля объема и качества выполняемой работы, обеспечения сохранности имущества и организационной деятельности Оператора.

3. Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

4. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между Оператором (организацией-работодателем) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

5. Сроки обработки и хранения персональных данных:

Обработка персональных данных, прекращается после окончания трудового договора работника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные работников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

С Положением об обработке и защите персональных данных Оператора ознакомлен(а).

**Настоящее согласие действует с «____» _____г.**

«___» _____ 201__ г. _____

(подпись)

**ПРИЛОЖЕНИЕ №2**
к Положению об обработке и защите персональных данных

**СОГЛАСИЕ**
**пациента на обработку персональных данных**

Я, нижеподписавшийся (аяся) _____
(Ф.И.О. полностью)
паспорт серия_____ номер _____ выдан _____дата выдачи _____
Адрес: _____
Телефон:_____

в соответствии с требованиями статьи 9 Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ, статьи 13 Федерального закона от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в РФ" подтверждаю свое согласие на обработку **Областное государственное бюджетное учреждение здравоохранения «Иркутская городская поликлиника № 11»** (664074 г. Иркутск ул. Лермонтова,89) (далее - Оператор) моих персональных данных, персональных данных представляемого мной _____(Ф.И.О.), включающих: фамилию, имя, отчество, пол, дату рождения, реквизиты документа удостоверяющего личность, адрес места жительства, адрес места регистрации, контактные телефоны, место работы, национальность, реквизиты полиса обязательного (добровольного) медицинского страхования застрахованного лица, страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью и другую информацию - в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг по договору, осуществление иных, связанных с этим мероприятий, а также в целях организации внутреннего учета Оператора, при условии сохранения врачебной тайны. В процессе оказания Оператором мне (представляемому мной лицу) медицинских услуг я предоставляю право медицинским работникам передавать мои персональные данные (персональные данные представляемого мной лица), в том числе составляющие врачебную тайну, другим должностным лицам Оператора в интересах моего обследования, лечения и внутреннего учета Оператора.

Предоставляю Оператору право осуществлять все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, передачу (в страховую медицинскую организацию, организацию -заказчика медицинских услуг в рамках заключенных договоров), обезличивание, блокирование, уничтожение.

Оператор вправе осуществлять следующие способы обработки персональных данных: на бумажных носителях, в информационных системах персональных данных с использованием и без использования средств автоматизации, а также смешанным способом.

**ПРИЛОЖЕНИЕ №3**
к Положению об обработке и защите
персональных данных

**ОТЗЫВ СОГЛАСИЯ**
на обработку персональных данных

Я, _____
*(фамилия, имя, отчество полностью)*

в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ "О персональных данных" отзываю у ОГБУЗ «ИГП № 11» согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в связи с

_____
*(указать причину)*

в срок, не превышающий тридцати дней с момента поступления настоящего отзыва.

«___» _____ 201__ г. _____ _____
(подпись) (расшифровка подписи)

**ПРИЛОЖЕНИЕ №4**

к Положению об обработке и защите персональных данных

**РАЗЪЯСНЕНИЕ**
**субъекту персональных данных юридических последствий отказа от предоставления своих персональных данных**

Уважаемый(ая) _____

В соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» разъясняем, что обязанность предоставления Вами персональных данных установлена

_____,
*(указывается пункт Федерального закона, его реквизиты и наименование)*
а также следующими нормативными актами

_____.
*(указываются реквизиты и наименования нормативных актов)*

В случае отказа Вами предоставить свои персональные данные
_____ не сможет на законных основаниях осуществить
_____,
*(указывается действие)*
что приведет к следующим для Вас юридическим последствиям:

_____
*(перечисляются юридические последствия для субъекта, то есть случаи возникновения, изменения или прекращения*

_____
*личных либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)*

С уважением,

_____ _____
(подпись) (расшифровка подписи)

**ПРИЛОЖЕНИЕ №5**

к Положению об обработке и защите персональных данных

**СОГЛАШЕНИЕ № _____**

о неразглашении конфиденциальной информации.

г. Иркутск « ____» _____20___ г.

Областное государственное бюджетное учреждение здравоохранения Иркутская городская поликлиника № 11, именуемое в дальнейшем ОГБУЗ «ИГП № 11» или «Поликлиника», в лице И.о. главного врача Поповой Ларисы Николаевны, действующей на основании распоряжения министерства здравоохранения Иркутской области от 09.01.2017 года № 2л/с, с одной стороны, и _____,

(ФИО)

зарегистрированный по адресу: г. Иркутск, ул. _____, д. ___, кв.___, паспорт РФ: серия _____ № _____, выдан «____»_____20___ г. _____

_____, именуемый(-ая) в дальнейшем «Работник», с другой стороны, совместно именуемые в дальнейшем «Стороны», заключили настоящее соглашение о нижеследующем.

1.Работник, в связи с исполнением своих должностных обязанностей, получает доступ к персональным данным сотрудников Поликлиники, иных лиц, участвующих в мероприятиях, организованных Поликлиникой, а также к сведениям, содержащим иную конфиденциальную информацию, доступ к которым ограничен Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и иными правовыми актами, и **обязуется не разглашать ставшие ему известными персональные данные сотрудников, иных лиц, иные сведения, содержащие конфиденциальную информацию**, за исключением случаев предусмотренных законодательством Российской Федерации.

2. Под конфиденциальной информацией в настоящем соглашении понимается речевая, аудиовизуальная, документированная информация с ограниченным доступом и иная информация, содержащая охраняемую в соответствии с действующим законодательством тайну Поликлиники, а также персональные данные сотрудников и обучающихся Поликлиники, иных лиц, участвующих в мероприятиях, организованных Поликлиникой. Конфиденциальная информация, содержащаяся в локальной сети Поликлиники, также имеет ограниченный доступ.

К конфиденциальной информации по настоящему соглашению в частности, но не ограничиваясь, относится любая или вся, настоящая или будущая, техническая, финансовая, деловая информация, статистика, данные, схемы, планы, спецификации, документы, идеи, концепции, продукты, процессы, технологии, цены, пароли доступа к информационным системам и другая информация, которая отнесена к конфиденциальной действующим законодательством Российской Федерации и локальными правовыми актами Поликлиники и была передана Работнику для выполнения последним своих трудовых обязанностей.

3. Не могут являться конфиденциальной информацией сведения:

- которые до момента заключения настоящего соглашения были публично обнародованы;
- которые стали общедоступны во время действия настоящего соглашения, но без виновного участия Работника.

4. Вся конфиденциальная информация, полученная Работником в материальной (схемы, рисунки, письма, фотографии и пр.) и нематериальной формах, является собственностью Поликлиники и используется только на условиях настоящего соглашения.

5. Работник обязуется:

5.1. Знать требования Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», «Положения об обработке и защите персональных данных» Поликлиники, «Положения о конфиденциальной информации и коммерческой тайне» Поликлиники.

5.2. Не разглашать и не передавать третьим лицам сведения, являющиеся конфиденциальной информацией, ставшие ему известными в связи с исполнением трудовых обязанностей, а также защищать вышеуказанные сведения от посягательств и попыток ее обнародовать третьими лицами.

5.3. Использовать сведения, полученные при исполнении своих трудовых обязанностей, лишь в интересах Поликлиники.

5.4. В случае увольнения из Поликлиники вернуть все сведения, полученные на материальных носителях, а также их копии, в течение одного дня с момента получения соответствующего требования о возврате.

5.5. Не использовать конфиденциальную информацию после увольнения из Поликлиники.

6. В случае разглашения Работником сведений, являющихся конфиденциальной информацией, трудовой договор с Работником подлежит расторжению в соответствии с подпунктом «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации.

7. В случае разглашения сведений, являющихся конфиденциальной информацией, Работник обязан в полном объеме возместить Поликлинике, понесенные в результате такого разглашения, убытки.

8. В случае разглашения конфиденциальной информации Работник может быть привлечен к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

9. Настоящее Соглашение действует бессрочно. Прекращение отношений по трудовому договору не является основанием для прекращения обязательств Сторон по настоящему соглашению.

10. Настоящее Соглашение составлено на двух страницах, на одном листе, в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой Стороны.

И.о. главного врача
ОГБУЗ «ИГП № 11» Работник

_____ Л.Н.Попова _____ /_____

М.П.

**ПРИЛОЖЕНИЕ №6**
к Положению об обработке и защите
персональных данных

## Журнал учета передачи персональных данных

| № | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Отметка о передаче или отказе в передаче персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**ПРИЛОЖЕНИЕ №7**
к Положению об обработке и защите персональных данных

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

| № | Сведения о запрашивающем лице | Краткое содержание обращения | Цель получения информации | Отметка о предоставлении или отказе в предоставлении информации | Дата передачи/отказа в предоставлении информации | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**ПРИЛОЖЕНИЕ №8**
к Положению об обработке и защите
персональных данных

**Акт приема-передачи документов (иных материальных носителей), содержащих персональные данные Работника**

Во исполнение договора оказания услуг № ____ от «___» _____ 20___ года, заключенного между ОГБУЗ «ИГП № 11», именуемым далее «Заказчик», в лице _____, действующего на основании _____, и _____ «_____», именуемым в дальнейшем «Исполнитель», в лице _____, действующего на основании Устава,

ЗАКАЗЧИК в лице _____ передает, а ИСПОЛНИТЕЛЬ в лице _____ получает документы (иные материальные носители), содержащие персональные данные Работника Заказчика _____ на срок _____ и в целях: _____
_____

**Перечень документов (иных материальных носителей), содержащих персональные данные Работника**

| № п/п | | Кол-во |
|---|---|---|
| | | |
| | | |
| Всего | | |

Полученные персональные данные Работника могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал _____
(Ф.И.О., должность работника, осуществляющего передачу персональных данных Работника)

_____
(ПОДПИСЬ)

Принял _____
(Ф.И.О., должность, представителя организации – приемщика документов (иных материальных носителей), содержащих персональные данные Работника)

_____
(ПОДПИСЬ)

**ПРИЛОЖЕНИЕ №9**
к Положению об обработке и защите
персональных данных

**Типовая форма**
**акта об уничтожении носителей, содержащих персональные данные**

Акт № _____
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и иной конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

| № п/п | Дата | **Тип носителя** | **Учетный номер носителя** | **Категория информации** | **Примечание** |
|---|---|---|---|---|---|
| | | | | | |

Всего носителей _____
*(цифрами и прописью количество)*

На указанных носителях персональные данные уничтожены путем
_____.
*(стирания на устройстве гарантированного уничтожения информации и т.п.)*

Перечисленные носители персональных данных уничтожены путем
_____.
*(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)*

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

**ПРИЛОЖЕНИЕ №10**
к Положению об обработке и защите персональных данных

**Журнал учета съемных носителей конфиденциальной информации (персональных данных)**

| № п/п | Регистрационный номер/дата | Тип/ёмкость машинного носителя персональных данных | Номер экземпляра/ количество экземпляров | Место установки (использования)/дата установки | Ответственное должностное лицо (ФИО) | Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата) |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| … | | | | | | | | | |
| N | | | | | | | | | |