

**Положение**  
**о защите, хранении, обработке и передаче персональных данных работников и пациентов**  
**ГК «Клиника профессора Кинзерского»**

1. Общие положения

1.1. Настоящее положение регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных) и иными нормативными правовыми актами в области обработки и защиты персональных данных.

1.2. Персональные данные работника - информация, необходимая ГК «Клиника профессора Кинзерского» (далее - медицинская организация, работодатель) в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные пациента - информация, полученная медицинской организацией при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг, а также информация, полученная в процессе оказания медицинской помощи.

1.3. К персональным данным работника относятся:

- фамилия, имя, отчество;
- пол;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- сведения об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ медицинского образования, о документах об образовании и (или) о квалификации, о договоре о целевом обучении, а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
- наименование организации, осуществляющей медицинскую деятельность;
- занимаемая должность в организации, осуществляющей медицинскую деятельность;
- сведения о членстве в медицинских профессиональных некоммерческих организациях;
- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

1.4. К персональным данным пациента относятся:

- фамилия, имя, отчество;
- пол;
- дата рождения;

- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- номер полиса обязательного медицинского страхования застрахованного лица;
- анамнез;
- диагноз;
- сведения об организации, осуществляющей медицинскую деятельность;
- вид оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
- результат обращения за медицинской помощью;
- серия и номер выданного листка нетрудоспособности;
- сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты;
- примененные клинические рекомендации;
- сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь, проводивших медицинские экспертизы, медицинские осмотры и медицинские освидетельствования;
- иные сведения, необходимые медицинской организации в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

1.5. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 статьи 13 Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

1.6. Все персональные сведения о работниках и пациентах медицинская организация может получить только от них самих. В случаях когда медицинская организация получает необходимые персональные данные работников и пациентов только у третьего лица, медицинская организация уведомляет об этом работников и пациентов и получает от них письменное согласие.

1.7. Медицинская организация сообщает работникам и пациентам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пациентов дать письменное согласие на их получение.

1.8. Персональные данные работников и пациентов являются конфиденциальной информацией и не могут быть использованы медицинской организацией или любым иным лицом в личных целях.

1.9. При определении объема и содержания персональных данных работников и пациентов медицинская организация руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

1.10. Медицинская организация разрабатывает меры защиты персональных данных работников и пациентов.

1.11. Работники и пациенты не должны отказываться от своих прав на неприкосновенность частной жизни.

2. Обработка, хранение и передача персональных данных работника и пациента

2.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.2. Обработка персональных данных пациента осуществляется исключительно в целях в медикопрофилактических целях, в целях установления медицинского диагноза, оказания медицинской помощи и медицинских услуг, оформления договорных отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну в соответствии с законодательством Российской Федерации.

2.3. Категория обрабатываемых персональных данных – специальная (персональные данные, касающиеся состояния здоровья).

2.4. Медицинская организация и Работодатель обрабатывает в информационных системах с использованием средств автоматизации персональные данные работников и пациентов, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных:

2.5. При 4-м уровне защищенности персональных данных медицинская организация:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

2.6. При 3-м уровне защищенности персональных данных медицинская организация дополнительно к мерам, перечисленным в пункте 2.5 настоящего положения, назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

2.7. При 2-м уровне защищенности персональных данных медицинская организация дополнительно к мерам, перечисленным в пунктах 2.5, 2.6 настоящего положения, ограничивает доступ к содержанию электронного журнала сообщений, за исключением для должностных лиц (работников), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

2.8. При 1-м уровне защищенности персональных данных медицинская организация дополнительно к мерам, перечисленным в пунктах 2.5-2.7 настоящего положения:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным, содержащимся в информационной системе;

- создает структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности.

2.9. Работодатель обрабатывает без использования средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту, которые хранятся на бумажных носителях:

- фамилия, имя, отчество;

- пол;

- дата и место рождения;

- гражданство;

- данные документа, удостоверяющего личность;

- место жительства;

- место регистрации;

- дата регистрации;

- страховой номер индивидуального лицевого счета;

- сведения об образовании;

2.10. Медицинская организация обрабатывает без использования средств автоматизации следующие категории персональных данных пациента, обеспечивает их защиту, которые хранятся на бумажных носителях:

- фамилия, имя, отчество;

- пол;

- дата рождения;

- данные документа, удостоверяющего личность;

- место жительства;

- место регистрации;

- дата регистрации;

- страховой номер индивидуального лицевого счета;

- номер полиса обязательного медицинского страхования застрахованного лица;

- анамнез;

- диагноз;

- иное.

2.11. Медицинская организация при обработке персональных данных работника или пациента на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;
- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников или пациентов.

2.12. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда медицинской организации, а документы, содержащие персональные данные пациентов, оформляются, ведутся и хранятся только лечащими врачами.

2.13. Работники отдела кадров, бухгалтерии, службы охраны труда, администраторы, диспетчеры колл центра, допущенные к персональным данным работников или пациентов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников или пациентов не допускаются.

2.14. Руководитель отдела кадров вправе передавать персональные данные работника в бухгалтерию организации в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.

2.15. Руководитель организации может передавать персональные данные работника третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных законодательством.

2.16. При передаче персональных данных работника руководитель отдела кадров и руководитель организации предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

2.17. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.18. Передача информации, содержащей сведения о персональных данных работников или пациентов, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

2.19. Персональные данные работника хранятся в отделе кадров, в сейфе на бумажных носителях: трудовая книжка, копии документов об образовании, трудовые договоры и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным работника имеют:

- руководитель организации;
- главный врач;
- заместители руководителя;

2.20. Персональные данные пациента хранятся в электронной базе данных «ИнфоКлиника», на бумажных носителях: договора, согласия, акты в Архиве и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным пациента имеют сотрудники согласно перечня должностей допущенных к работе с персональными данными.

2.21. Медицинская организация осуществляет передачу персональных данных работников и пациентов только при наличии согласия указанных лиц на обработку персональных данных, разрешенных ими для распространения.

2.22. Согласие работника или пациента на обработку персональных данных, разрешенных ими для распространения, оформляется отдельно от иных согласий указанного лица на обработку его персональных данных.

2.23. Медицинская организация обеспечивает работникам и пациентам возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных этими лицами для распространения.

2.24. Молчание или бездействие работника или пациента ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных им для распространения.

2.25. В согласии работника или пациента на обработку персональных данных, разрешенных им для распространения, работник или пациент вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных медицинской организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Отказ медицинской организации в установлении работником или пациентом запретов и условий, предусмотренных в настоящем пункте, не допускается.

2.26. Медицинская организация в срок не позднее трех рабочих дней с момента получения соответствующего согласия работника или пациента публикует информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных этим работником или пациентом для распространения.

2.27. Установленные работником или пациентом запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных им для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

2.28. Все сведения о передаче персональных данных работников и пациентов учитываются для контроля правомерности использования данной информации лицами, ее получившими.

2.29. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается только в случаях, если работник или пациент дал согласие в письменной форме на обработку своих персональных данных или персональные данные сделаны общедоступными самим субъектом персональных данных.

3. Требования к помещениям, в которых производится обработка персональных данных

3.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

3.3. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

3.4. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

4. Обязанности медицинской организации по хранению и защите персональных данных работников и пациентов

4.1. Медицинская организация за свой счет обеспечивает защиту персональных данных работников и пациентов от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации.

4.2. Медицинская организация принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. Медицинская организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, относятся:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих политику медицинской организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на медицинскую организацию не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике медицинской организации в отношении обработки персональных данных, ее локальным актам;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых медицинской организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных названным Федеральным законом;

6) ознакомление работников медицинской организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику медицинской организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.3. Медицинская организация знакомит работников и их представителей с настоящим положением и их правами в области защиты персональных данных под расписку.

4.4. Медицинская организация осуществляет передачу персональных данных работников и пациентов только в соответствии с настоящим положением и законодательством Российской Федерации.

4.5. Медицинская организация предоставляет персональные данные работников и пациентов только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим положением и законодательством Российской Федерации.

4.6. Медицинская организация не вправе предоставлять персональные данные работников и пациентов в коммерческих целях без их письменного согласия.

4.7. Медицинская организация обеспечивает работникам и пациентам свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

4.8. Медицинская организация по требованию работника и пациента предоставляет ему полную информацию о его персональных данных и обработке этих данных.

5. Права работников и пациентов на защиту их персональных данных

5.1. Работник или пациент в целях обеспечения защиты своих персональных данных, хранящихся в медицинской организации, имеют право:

- получать полную информацию о своих персональных данных, их обработке, хранении и передаче;
- определять своих представителей для защиты своих персональных данных;
- на доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по их выбору;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями настоящего положения и законодательства Российской Федерации.

При отказе медицинской организации исключить или исправить его персональные данные работник или пациент вправе заявить в письменном виде о своем несогласии с соответствующим обоснованием;

- требовать от медицинской организации извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника или пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2. Если работник или пациент считает, что медицинская организация осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы, работник или пациент вправе обжаловать действия или бездействие медицинской организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5.3. Работник или пациент вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных им для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Закона о персональных данных или обратиться с таким требованием в суд.

## 6. Порядок уничтожения, блокирования персональных данных

6.1. В случае выявления неправомерной обработки персональных данных при обращении работника или пациента медицинская организация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому работнику или пациенту, с момента такого обращения на период проверки.

6.2. В случае выявления неточных персональных данных при обращении работника или пациента медицинская организация осуществляет блокирование персональных данных, относящихся к этому работнику или пациенту, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы работника или пациента, или третьих лиц.

6.3. В случае подтверждения факта неточности персональных данных медицинская организация на основании сведений, представленных работником или пациентом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.4. В случае поступления требования работника или пациента о прекращении распространения его персональных данных передача (распространение, предоставление, доступ) персональных данных, разрешенных таким работником или пациентом для распространения, должна быть прекращена в течение трех рабочих дней с момента получения такого требования.

Действие согласия работника или пациента на обработку персональных данных, разрешенных им для распространения, прекращается с момента поступления в медицинскую организацию указанного требования.

6.5. В случае выявления неправомерной обработки персональных данных, осуществляемой медицинской организацией, медицинская организация в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

6.6. В случае если обеспечить правомерность обработки персональных данных невозможно, медицинская организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

6.7. Об устранении допущенных нарушений или об уничтожении персональных данных медицинская организация уведомляет работника или пациента.

6.8. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав работника или пациента, медицинская организация с момента выявления такого инцидента медицинской организацией, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав работника или пациента, и предполагаемом вреде, нанесенном правам работника или пациента, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном медицинской организацией на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.9. В случае достижения цели обработки персональных данных медицинская организация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором или договором на оказание медицинских услуг.

6.10. В случае отзыва работником или пациентом согласия на обработку его персональных данных медицинская организация прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором или договором на оказание медицинских услуг.

6.11. В случае обращения работника или пациента в медицинскую организацию с требованием о прекращении обработки персональных данных медицинская организация в срок, не превышающий десяти рабочих дней с даты получения ей соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления медицинской организацией в адрес работника или пациента мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.12. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.11 настоящего положения, медицинская организация осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.13. После истечения срока нормативного хранения документов, содержащих персональные данные работника или пациента, или при наступлении иных законных оснований документы подлежат уничтожению.

6.14. Медицинская организация для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

6.15. По результатам экспертизы документы, содержащие персональные данные работника или пациента и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем сжигания;

- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников и пациентов

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника или пациента, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством Российской Федерации.

7.2. Моральный вред, причиненный работнику или пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником или пациентом убытков.

8. Заключительные положения

8.1. Настоящее положение вступает в силу с момента издания приказа о его утверждении

8.2. Медицинская организация обеспечивает неограниченный доступ к настоящему документу.

8.3. Настоящее положение доводится до сведения всех работников посредством общего собрания.