Утверждено приказом ИП Прудко Максим Юрьевич
№ Б/Н от 02.09.2025 года

Положение о защите, хранении, обработке и передаче персональных данных работников и пациентов ИП Прудко Максим Юрьевич (стоматология «Доктор Потанова»)

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о ПДн) и иными нормативными правовыми актами в области обработки и защиты персональных данных.

1.2. Персональные данные работника (соискателя) – информация, необходимая ИП Прудко М.Ю. (далее – медицинская организация, работодатель) в связи с трудовыми отношениями и касающаяся конкретного работника (соискателя). Персональные данные пациента – информация, полученная медицинской организацией при первоначальном обращении 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 (СНИЛС);
- 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;
- сведения о членстве в медицинских профессиональных некоммерческих организациях;
- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации, 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 (СНИЛС);
- номер полиса обязательного медицинского страхования;
- анамнез;
- диагноз;
- состояние здоровья;
- фотографии;
- видеозаписи;
- иные данные, необходимые для оказания медицинской помощи.

1.5. Все персональные сведения о работниках и пациентах медицинская организация получает только от них самих. В случаях, когда необходимые персональные данные можно получить только от третьего лица, медицинская организация уведомляет об этом работника или пациента и получает от них письменное согласие.

1.6. 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 дать письменное согласие на их получение.

1.7. Персональные данные работников и пациентов являются конфиденциальной информацией и не могут быть использованы медицинской организацией или любым иным лицом без согласия субъекта, за исключением случаев, предусмотренных федеральными законами.

1.8. При определении объёма и содержания обрабатываемых персональных данных медицинская организация руководствуется настоящим Положением, Конституцией РФ, Трудовым кодексом РФ, иными федеральными законами.

1.9. Медицинская организация разрабатывает и принимает необходимые меры защиты персональных данных.

1.10. 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 обеспечения соблюдения законов, установления медицинского диагноза и оказания медицинских услуг.

2.3. Работодатель обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту с учётом определённого типа угроз безопасности и уровня защищённости персональных данных:

Цель обработки: ведение кадрового делопроизводства.

Категория персональных данных	Перечень персональных данных	Категория работников	Тип угрозы	Уровень защищённости	Срок обработки и хранения
общие персональные данные	фамилия, имя, отчество; пол; дата и место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; СНИЛС; сведения об образовании	все работники	угрозы 3 типа	4 уровень защищённости	в соответствии с законодательством

2.4. Медицинская организация обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных пациента:

Цель обработки: оказание медицинских услуг.

Категория персональных данных	Перечень персональных данных	Категория пациентов	Тип угрозы	Уровень защищённости	Срок обработки и хранения
общие, специальные и биометрические персональные данные	фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; СНИЛС; номер полиса ОМС; анамнез; диагноз; состояние здоровья; фото; видео; иное	все пациенты	угрозы 3 типа	4 уровень защищённости	5 лет

2.5. При 4-м уровне защищённости персональных данных медицинская организация:
- обеспечивает режим безопасности помещений, в которых размещена информационная система, предотвращающий возможность неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа;
- обеспечивает сохранность носителей персональных данных;
- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения 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 защищённости дополнительно назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе.

2.7. При 2-м уровне защищённости дополнительно организуется доступ к содержанию электронного журнала сообщений только для должностных лиц, которым эти сведения необходимы для выполнения служебных обязанностей.

2.8. При 1-м уровне защищённости дополнительно:
- обеспечивается автоматическая регистрация в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным;
- создаётся структурное подразделение или возлагаются на одно из подразделений функции по обеспечению безопасности персональных данных.

2.9. Работодатель обрабатывает без использования средств автоматизации следующие категории персональных данных работника на бумажных носителях:

Цель обработки: ведение кадрового делопроизводства.

Категория персональных данных	Перечень персональных данных	Категория работников	Срок обработки и хранения
общие персональные данные	фамилия, имя, отчество; пол; дата и место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; СНИЛС; сведения об образовании; иное	все работники	в соответствии с законодательством

2.10. Медицинская организация обрабатывает без использования средств автоматизации следующие категории персональных данных пациента на бумажных носителях:

Цель обработки: оказание медицинских услуг.

Категория персональных данных	Перечень персональных данных	Категория пациентов	Срок обработки и хранения
общие, специальные и биометрические персональные данные	фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; СНИЛС; номер полиса ОМС; анамнез; диагноз; состояние здоровья; фото; видео; иное	все пациенты	5 лет

2.11. При обработке персональных данных на бумажных носителях медицинская организация:
- назначает должностное лицо, ответственное за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, содержащие персональные данные.

2.12. Документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и специалистом по охране труда. Документы, содержащие персональные данные пациентов, оформляются, ведутся и хранятся только лечащими врачами и медицинским персоналом.

2.13. Работники, допущенные к персональным данным, подписывают обязательство о неразглашении. Без подписания такого обязательства они не допускаются к обработке персональных данных.

2.14. Руководитель отдела кадров вправе передавать персональные данные работника в бухгалтерию в случаях, установленных законодательством.

2.15. Руководитель организации может передавать персональные данные работника третьим лицам только для предупреждения угрозы жизни и здоровью работника, а также в иных случаях, предусмотренных законом.

2.16. При передаче персональных данных работника уполномоченные лица предупреждают получателей о том, что данные могут быть использованы лишь в целях, для которых они сообщены, и требуют письменного подтверждения соблюдения этого условия.

2.17. Передача персональных данных по запросам третьих лиц, если она прямо не предусмотрена законодательством, допускается только с согласия работника (пациента) на обработку его персональных данных.

2.18. Передача информации, содержащей персональные данные, по телефону (в связи с невозможностью идентификации лица) запрещается.

2.19. Персональные данные работника хранятся в отделе кадров в сейфе (на бумажных носителях: трудовая книжка, личная карточка) и на электронных носителях с ограниченным доступом.
Право доступа к персональным данным работника имеют:
- руководитель организации;
- руководитель отдела кадров;
- сотрудники отдела кадров;
- специалист по охране труда.

2.20. Персональные данные пациента хранятся в запираемых шкафах (медицинские карты) и на электронных носителях с ограниченным доступом.
Право доступа к персональным данным пациента имеют: ИП Прудко М.Ю., медицинские работники, администраторы (в объёме, необходимом для исполнения должностных обязанностей).

2.21. Передача персональных данных работников и пациентов осуществляется только при наличии согласия указанных лиц на обработку персональных данных, разрешённых ими для распространения.

2.22. Согласие на обработку персональных данных, разрешённых для распространения, оформляется отдельно от иных согласий.

2.23. Медицинская организация обеспечивает субъектам возможность определить перечень персональных данных по каждой категории, указанной в согласии на распространение.

2.24. Молчание или бездействие субъекта не может считаться согласием на обработку персональных данных, разрешённых для распространения.

2.25. В согласии субъект вправе установить запреты на передачу (кроме предоставления доступа) неограниченному кругу лиц, а также запреты на обработку или условия обработки неограниченным кругом лиц.

2.26. Медицинская организация в срок не позднее трёх рабочих дней с момента получения согласия публикует информацию об условиях обработки и о наличии запретов.

2.27. Установленные запреты не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определённых законодательством.

2.28. Все сведения о передаче персональных данных учитываются для контроля правомерности использования информации.

2.29. Обработка специальных категорий персональных данных (о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни) допускается только при наличии письменного согласия субъекта или если данные сделаны общедоступными самим субъектом.

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

3.1. Размещение оборудования информационных систем персональных данных, специального оборудования, организация режима безопасности в помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения посторонних лиц.

3.2. Помещения должны соответствовать требованиям пожарной безопасности, установленным законодательством РФ.

3.3. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией с составлением актов.

3.4. При использовании криптографических средств защиты информации реализуются дополнительные требования согласно методическим документам ФСБ России.

4. Обязанности медицинской организации по хранению и защите персональных данных

4.1. Медицинская организация за свой счёт обеспечивает защиту персональных данных от неправомерного использования или утраты в порядке, установленном законодательством.

4.2. Медицинская организация принимает необходимые и достаточные меры для выполнения обязанностей, предусмотренных Законом о ПДн, в том числе:
1) назначает ответственного за организацию обработки персональных данных;
2) издаёт локальные акты по вопросам обработки персональных данных (политику, перечни, порядок уничтожения и т.д.);
3) применяет правовые, организационные и технические меры по обеспечению безопасности;
4) осуществляет внутренний контроль и аудит соответствия обработки;
5) оценивает возможный вред и соразмерность принимаемых мер;
6) знакомит работников, непосредственно осуществляющих обработку, с положениями законодательства и локальными актами.

4.3. Медицинская организация знакомит работников и их представителей с настоящим Положением под расписку.

4.4. Передача персональных данных осуществляется только в соответствии с Положением и законодательством.

4.5. Предоставление персональных данных уполномоченным лицам – только в объёме, необходимом для выполнения их трудовых обязанностей.

4.6. Использование персональных данных в коммерческих целях без письменного согласия запрещено.

4.7. Обеспечивается свободный бесплатный доступ субъектов к своим персональным данным и получение копий записей, за исключением случаев, предусмотренных законом.

4.8. По требованию субъекта предоставляется полная информация о его персональных данных и их обработке.

5. Права работников и пациентов на защиту их персональных данных

5.1. Субъект персональных данных имеет право:
- получать полную информацию о своих данных, их обработке и передаче;
- определять представителей для защиты своих прав;
- на доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору;
- требовать исключения или исправления неверных или неполных данных;
- требовать извещения всех лиц, которым ранее были сообщены неверные данные, о внесённых изменениях.

5.2. В случае нарушения прав субъект вправе обжаловать действия медицинской организации в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в суд.

5.3. Субъект вправе требовать прекращения передачи своих персональных данных, ранее разрешённых для распространения, если нарушаются положения Закона о ПДн.

6. Порядок уничтожения, блокирования персональных данных

6.1. При выявлении неправомерной обработки персональных данных по обращению субъекта медицинская организация блокирует такие данные на период проверки.

6.2. При выявлении неточных данных они блокируются на период проверки, если это не нарушает права и законные интересы субъекта или третьих лиц.

6.3. При подтверждении неточности данных они уточняются в течение 7 рабочих дней со дня представления необходимых сведений, после чего блокирование снимается.

6.4. При поступлении требования о прекращении распространения персональных данных передача должна быть прекращена в течение 3 рабочих дней. Действие согласия на распространение прекращается с момента поступления требования.

6.5. При выявлении неправомерной обработки медицинская организация прекращает её в срок не более 3 рабочих дней.

6.6. Если обеспечить правомерность обработки невозможно, персональные данные уничтожаются в срок не более 10 рабочих дней.

6.7. Об устранении нарушений или уничтожении данных уведомляется субъект.

6.8. При неправомерной или случайной передаче, повлёкшей нарушение прав субъектов, медицинская организация уведомляет Роскомнадзор:
- в течение 24 часов – об инциденте, предполагаемых причинах и принятых мерах;
- в течение 72 часов – о результатах внутреннего расследования.

6.9. При достижении цели обработки персональные данные уничтожаются в срок не более 30 дней, если иное не предусмотрено договором.

6.10. При отзыве согласия на обработку обработка прекращается, и данные уничтожаются в срок не более 30 дней, если иное не предусмотрено договором.

6.11. При обращении с требованием о прекращении обработки (если это не противоречит закону) обработка прекращается в срок не более 10 рабочих дней (может быть продлён с уведомлением, но не более чем на 5 дней).

6.12. При невозможности уничтожения в установленные сроки данные блокируются и уничтожаются в срок не более 6 месяцев, если иное не установлено федеральными законами.

6.13. После истечения срока хранения документы подлежат уничтожению.

6.14. Для уничтожения создаётся экспертная комиссия, проводится экспертиза ценности документов.

6.15. Уничтожение бумажных документов производится с помощью шредера; электронные данные стираются или носители физически уничтожаются.

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

7.1. Лица, виновные в нарушении норм, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством РФ.

7.2. Моральный вред, причинённый субъекту вследствие нарушения его прав, подлежит возмещению независимо от возмещения имущественного вреда и понесённых убытков.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения.

8.2. Медицинская организация обеспечивает неограниченный доступ к настоящему документу (размещение на информационных стендах, официальном сайте и т.п.).

8.3. Положение доводится до сведения всех работников персонально под подпись.