УТВЕРЖДЕН

Приказом Генерального директора
ТОО «Medium clinic»
№ 01 – А от 6 января 2025 года

ПОЛОЖЕНИЕ

Положение о персональных данных ТОО «Medium clinic»

г. Алматы

Положение о персональных данных в Товариществе с ограниченной ответственностью "Medium Clinic"

1. Общие положения

1.1. Настоящее Положение о персональных данных (далее – Положение) в Товариществе с ограниченной ответственностью "Medium Clinic" (далее – «Товарищество», «Компания») разработано в соответствии с Конституцией Республики Казахстан, Трудовым кодексом Республики Казахстан, Законом Республики Казахстан «О персональных данных и их защите», а также иными нормативными правовыми актами Республики Казахстан и внутренними нормативными актами Компании, с учетом специфики медицинской деятельности.
1.2. Положение регулирует порядок сбора, обработки (накопления, хранения, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения) и защиты персональных данных, в том числе данных о здоровье, в Компании, а также гарантии обеспечения их конфиденциальности в соответствии с действующим законодательством Республики Казахстан.

2. Основные понятия

2.1. В настоящем Положении используются следующие понятия:

- **Персональные данные** – любые сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе, включая, но не ограничиваясь, ФИО, ИИН, дата рождения, место работы, должность, номер телефона, электронная почта, место жительства, а также медицинская информация (диагнозы, результаты анализов, история болезни).
- **Особо чувствительные персональные данные** – данные, относящиеся к здоровью субъекта, включая медицинские карты, результаты обследований, диагнозы, рецепты и иную информацию, которую закон требует обрабатывать в особом порядке.
- **Медицинская информация** – любые данные, относящиеся к физическому и психическому состоянию здоровья субъекта, в том числе результаты диагностики, лечение, хирургические вмешательства, медицинские назначения и показания.
- **Обработка персональных данных** – любые действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных, включая персональные данные о здоровье.

3. Цели обработки персональных данных

3.1. Компания осуществляет сбор, обработку и защиту персональных данных с целью:

- Обеспечения медицинского обслуживания клиентов, включая ведение медицинских карт, предоставление диагностических и лечебных услуг.
- Организации трудовых отношений с Работниками (в том числе для оформления медицинского страхования, предоставления отпусков по болезни и т.д.).
- Обеспечения выполнения обязательств перед государственными органами, включая предоставление сведений о сотрудниках в Пенсионный фонд, Фонд социального медицинского страхования и другие органы.
- Оформление договоров с контрагентами и партнерами, включая выполнение медицинских услуг.
- Формирования статистической отчетности по вопросам здравоохранения, в том числе для предоставления в государственные органы.
- Организации мероприятий для повышения качества медицинских услуг и безопасности пациентов, в том числе на основе аналитики данных.

4. Сбор и обработка персональных данных

4.1. Сбор, обработка и защита персональных данных, включая медицинские, могут осуществляться на основании следующих оснований:

- Согласие субъекта персональных данных (в том числе на обработку данных о здоровье).
- Необходимость для выполнения медицинского обслуживания, включая диагностику, лечение, ведение медицинской документации.
- Соблюдение обязательств перед государственными органами (например, отчетность в Фонд социального медицинского страхования).
- Защита жизненно важных интересов субъекта (например, в случае экстренной медицинской помощи).
- Исполнение трудовых и иных договорных обязательств.

4.2. Особое внимание уделяется защите медицинской информации, которая классифицируется как особо чувствительные персональные данные, с применением более строгих мер безопасности.

5. Защита персональных данных

5.1. Компанией принимаются следующие меры для обеспечения защиты персональных данных, в том числе медицинских данных:

- Хранение персональных данных, включая данные о здоровье, только в защищенных и зашифрованных базах данных.
- Обеспечение конфиденциальности медицинской информации, включая соблюдение строгих процедур доступа для персонала, работающего с такими данными.
- Использование средств криптографической защиты информации для хранения и передачи данных.
- Ограничение доступа к персональным данным, в том числе медицинским, на основе принципа необходимости (доступ предоставляется только тем сотрудникам, которые напрямую взаимодействуют с данными для выполнения своих рабочих обязанностей).
- Применение антивирусных программ и других средств защиты от несанкционированного доступа.

5.2. Принципы работы с персональными данными включают:

- Минимизация сбора персональных данных: собираются только те данные, которые необходимы для конкретных целей (например, для предоставления медицинской помощи или выполнения трудовых обязанностей).
- Точность и актуальность данных: персональные данные, в том числе медицинские, должны быть точными и актуальными.
- Ожидаемое время хранения данных: персональные данные хранятся только в течение необходимого срока, в соответствии с законодательными требованиями.

6. Обработка медицинских данных

6.1. Обработка медицинских данных, таких как результаты диагностики, лечебные назначения и другие данные о здоровье пациента, осуществляется с обязательным соблюдением всех требований конфиденциальности и с использованием только уполномоченных специалистов.

6.2. Медицина требует особой защиты данных о здоровье. Вся медицинская информация, связанная с пациентами, должна обрабатываться и храниться в условиях, исключающих несанкционированный доступ, с применением технологий шифрования.

6.3. Врачи и медицинский персонал обязаны информировать пациентов о целях обработки их персональных данных и получать явное согласие на обработку таких данных.

7. Хранение персональных данных

7.1. Хранение персональных данных в Компании осуществляется как на бумажных носителях (например, медицинские карты), так и на электронных носителях (медицинские системы, базы данных).
7.2. Бумажные носители персональных данных (медицинские карты, медицинские отчеты и пр.) хранятся в специально оборудованных местах с ограниченным доступом, которые защищены от несанкционированного доступа.
7.3. Электронные носители персональных данных (включая данные о здоровье) хранятся на защищенных серверах, в зашифрованных базах данных, с использованием современных средств защиты информации.
7.4. Обработка персональных данных, включая данные о здоровье, может осуществляться только с применением систем, расположенных на территории Республики Казахстан.

8. Доступ к персональным данным

8.1. Доступ к персональным данным, в том числе к медицинской информации, имеет только те сотрудники, чьи обязанности напрямую связаны с обработкой таких данных.
8.2. В случае увольнения или перевода сотрудника, не имеющего отношения к обработке персональных данных, доступ к этим данным должен быть немедленно прекращен.

9. Ответственность за нарушение норм

9.1. Лица, виновные в нарушении норм по обработке персональных данных, несут ответственность в соответствии с законодательством Республики Казахстан, включая дисциплинарную, административную, гражданско-правовую и уголовную ответственность.
Для полноценной защиты как **работников**, так и **пациентов**, важно дополнить Положение соответствующими мерами, которые обеспечат соблюдение их прав на конфиденциальность, безопасность их персональных данных и защиту от возможных рисков. Следующие дополнения касаются защиты **работников** и **пациентов**, включая более подробные аспекты безопасности данных и меры, направленные на защиту их прав.

10. Защита персональных данных работников

10.1.**Сбор, обработка и защита персональных данных работников** осуществляется в соответствии с принципами законности, справедливости и прозрачности, а также с соблюдением прав работников на конфиденциальность их данных. Все персональные данные, включая медицинские и трудовые, обрабатываются только в рамках установленных целей, например, для

обеспечения трудовых правоотношений, предоставления медицинского страхования, начисления выплат и т.д.

10.2. **Особая защита данных о здоровье работников**:

- Для обеспечения их прав на медицинскую конфиденциальность, все данные, относящиеся к состоянию здоровья работников, такие как результаты обследований, диагнозы, медицинские карты, должны храниться в защищенном формате и быть доступными только для уполномоченных сотрудников.
- Медицинская информация о здоровье работников обрабатывается только с их явного согласия, за исключением случаев, когда обработка данных необходима для обеспечения их прав в области трудового законодательства (например, оформление больничных листов).

10.3. **Меры по защите персональных данных работников**:

- Установление строгих ограничений на доступ к персональным данным работников, включая использование многослойных систем безопасности (например, двухфакторной аутентификации).
- Обучение сотрудников, имеющих доступ к персональным данным, принципам защиты данных, а также ответственности за нарушение конфиденциальности.

10.4. **Защита данных при увольнении**:

- При увольнении или переводе работника на другую должность, доступ к его персональным данным, включая информацию о здоровье, должен быть немедленно прекращен.
- Все документы, содержащие персональные данные, включая медицинские, должны быть переданы в соответствующие отделы для дальнейшего хранения или уничтожения в соответствии с внутренними регламентами.

11. Защита персональных данных пациентов

11.1. **Сбор и обработка персональных данных пациентов** (в том числе данные о здоровье) осуществляется исключительно с их явного согласия. Пациенты должны быть проинформированы о целях сбора данных, а также о том, как и кем эти данные будут обрабатываться. Согласие на обработку данных должно быть документально подтверждено, а информация о целях и сроках хранения данных – доступна пациенту.

11.2. **Защита медицинской конфиденциальности пациентов**:

- Все медицинские данные пациентов, включая информацию о диагнозах, истории болезни, результаты анализов, рецепты и назначения, являются конфиденциальными и могут быть раскрыты только уполномоченным лицам в случае необходимости, например, при экстренном лечении.
- Для защиты данных пациентов в электронной форме используются системы шифрования, а также механизмы контроля доступа, чтобы

только уполномоченные медицинские работники имели доступ к медицинской информации.

11.3. **Обработка медицинских данных**:

- Обработка медицинских данных о пациентах осуществляется только в тех случаях, когда это необходимо для диагностики, лечения или других медицинских процедур.
- В случае необходимости предоставления данных третьим лицам (например, для выполнения обязательного медицинского страхования или в случае обращения в органы государственного контроля), персональные данные передаются только в строго ограниченных случаях и при наличии юридических оснований.

11.4. **Информированное согласие пациента**:

- Перед оказанием медицинской помощи пациенту предоставляется вся необходимая информация о том, какие данные будут собираться и как они будут использоваться, включая информацию о праве на отказ от предоставления данных.
- В случае предоставления согласия, пациент должен быть проинформирован о сроках хранения его данных и процедуре их уничтожения после завершения лечения или в случае отказа от услуг.

11.5. **Особая защита данных несовершеннолетних пациентов**:

- Для несовершеннолетних пациентов обработка персональных данных возможна только с согласия их законных представителей (родителей или опекунов).
- Все данные о здоровье несовершеннолетних пациентов должны обрабатываться с повышенными мерами конфиденциальности и защищенности.

12. Обязанности сотрудников компании по защите данных работников и пациентов

12.1. **Соблюдение конфиденциальности персональных данных**:

- Все сотрудники Компании обязаны соблюдать требования конфиденциальности, не разглашать и не использовать персональные данные работников и пациентов в личных целях.
- Работники Компании, имеющие доступ к персональным данным, проходят обучение по вопросам защиты информации и обязаны подписывать обязательство о конфиденциальности.

12.2. **Меры по предотвращению утечек данных**:

- Для защиты персональных данных от несанкционированного доступа, утечек, повреждений или уничтожения компания использует современные технические средства защиты информации, такие как антивирусное ПО, системы обнаружения вторжений, брандмауэры.

- В случае утечки данных или попытки несанкционированного доступа к ним, должны быть немедленно приняты меры по минимизации ущерба и информированию пострадавших субъектов данных.

12.3. **Использование персональных данных в научных целях**:

- В случае использования персональных данных работников или пациентов для научных исследований или статистических целей, данные должны быть обезличены, чтобы исключить возможность идентификации конкретного субъекта данных.
- Пациенты и работники должны быть информированы о возможном использовании их данных в научных целях и дать на это согласие.

13. Ответственность за нарушение конфиденциальности персональных данных

13.1. Лица, нарушившие требования по защите персональных данных работников или пациентов, несут дисциплинарную, административную, гражданско-правовую и/или уголовную ответственность в соответствии с законодательством Республики Казахстан.

13.2. За утечку или несанкционированный доступ к персональным данным, включая медицинские данные, работники Компании могут быть подвергнуты дисциплинарным взысканиям вплоть до увольнения, а также могут быть привлечены к юридической ответственности, если их действия привели к ущербу для субъектов персональных данных.

14. Права субъектов персональных данных

14.1. **Права работников и пациентов**:

- Каждый работник и пациент имеет право на доступ к своим персональным данным, включая медицинские данные, а также на запрос их исправления или удаления в случае ошибки или изменения информации.
- Пациенты и работники могут в любое время отозвать свое согласие на обработку персональных данных, за исключением случаев, когда продолжение обработки данных необходимо для выполнения обязательств перед государственными органами или для соблюдения иных законных оснований.

14.2. **Право на безопасность**:

- Все субъекты персональных данных имеют право требовать от Компании обеспечения их безопасности и защиты их данных от незаконного использования, утечек или других угроз.
- В случае утечки данных или другого инцидента, связанного с нарушением безопасности персональных данных, Компания обязана

немедленно уведомить пострадавших субъектов данных и предпринять все необходимые шаги для минимизации ущерба.

15. Уничтожение персональных данных

Персональные данные должны быть уничтожены в случае наступления одного из следующих событий:

- истечения срока хранения персональных данных в соответствии с законодательством Республики Казахстан;
- окончания договорных или других правоотношений между Компанией, Собственник, и (или) Субъектом, и (или) третьим лицом;
- вступления в законную силу решения суда в соответствии с действующим законодательством Республики Казахстан;
- в иных случаях, установленных законодательством Республики Казахстан.