ПОЛОЖЕНИЕ
о персональных данных пациентов

1. Общие положения

1.1. Настоящее Положение определяет порядок обработки (получения, использования, хранения, уточнения (обновления, изменения), распространения (в том числе передачи), обезличивания, блокирования, уничтожения, защиты) персональных данных пациентов ТОО «Diamond Star», а также гарантии обеспечения конфиденциальности сведений о них.

1.2. Настоящее Положение разработано в соответствии с Гражданским кодексом РК, законом «О защите прав потребителей», Правилами предоставления медицинскими организациями платных медицинских услуг ("Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг"), Кодексом РК "О здоровье народа и системе здравоохранения".

1.3. Требования настоящего Положения распространяются на всех работников ТОО «Diamond Star» .

2. Основные понятия, обозначения

В настоящем Положении используются следующие понятия и термины:

Работник — физическое лицо, вступившее в трудовые отношения с работодателем;

Работодатель – ТОО «Diamond Star», далее по тексту – **Организация**.

Пациенты- лица, обратившиеся за оказанием медицинских услуг в Организацию.

Субъекты персональных данных — пациенты, работники Организации, третьи лица.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, информация, составляющая врачебную тайну и другая информация, необходимая Организации в связи с организацией оказания платных медицинских услуг.

Врачебная тайна - Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, (в соответствии с Кодексом РК "О здоровье народа и системе здравоохранения").

Оператор – Организации и должностные лица Организации, организующие и (или) осуществляющие обработку персональных данных;

Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), защиту, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы субъекта персональных данных или других лиц;

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
Информационная система персональных данных — информационная система, представляющая 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;
Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
Конфиденциальность персональных данных — обязательное для соблюдения должностным лицом Организации, иным лицам, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
Информация — сведения (сообщения, данные) независимо от формы их представления;
Доступ к информации — возможность получения информации и ее использования.

3. Цели и задачи
3.1. Целями настоящего Положения выступают:
3.1.1 обеспечение соответствия законодательству РК действий работников Организации, направленных на обработку персональных данных пациентов, третьих лиц (других граждан);
3.1.2 обеспечение защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.
3.2. Задачами настоящего Положения являются:
3.2.1 определение принципов, порядка обработки персональных данных;
3.2.2 определение условий обработки персональных данных, способов защиты персональных данных;
3.2.3 определение прав и обязанностей Организации и субъектов персональных данных при обработке персональных данных.

4. Понятие и состав персональных данных
4.1. Персональные данные включают в себя: фамилию, имя, отчество, дату и место рождения, должность, место работы, сведения об образовании, ученую степень, звание, паспортные данные, место жительства, контактные телефоны, адрес электронной почты, сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, номер страхового медицинского полиса, семейное положение, состав семьи.

4.2. Организация осуществляет обработку персональных данных следующих категорий субъектов:

- работников, состоящих в трудовых отношениях с Организацией;
- пациентов Организации;
- иных физических лиц, данные о которых обрабатываются во исполнение уставных задач Организации.

4.3. Информация о персональных данных может содержаться:

- на бумажных носителях;
- на электронных носителях;
- в информационно-телекоммуникационных сетях и иных информационных системах.

4.4. Организация использует следующие способы обработки персональных данных:

- автоматизированная обработка;
- без использования средств автоматизации;
- смешанная обработка (с применением объектов вычислительной техники).

Организация самостоятельно устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей Организации.

При обработке персональных данных с применением объектов вычислительной техники должностные лица, осуществляющие такую обработку (пользователи объектов вычислительной техники), должны быть ознакомлены под роспись с локальными нормативными актами Организации, устанавливающими порядок применения объектов вычислительной техники в Организации.

4.5. Персональные данные пациентов Организации содержатся в следующих документах (копиях указанных документов):

а) медицинская документация на имя пациента (медицинская карта пациента и ее приложения, медицинские справки, результаты анализов, врачебно-консультативное заключение, протоколы заседания ВК и пр.)

б) договор на оказание платных медицинских услуг и его приложения;

в) другие документы, содержащие персональные данные и предназначенные для использования в служебных целях.

5. Создание и обработка персональных данных

5.1. Создание персональных данных

Документы, содержащие персональные данные, создаются путём:

а) копирования оригиналов (удостоверение личности, свидетельство ИНН, свидетельство государственного пенсионного страхования, страховой медицинский полюс др.);

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

5.2. Основы организации обработки персональных данных в Организации (цели, принципы, правовые основы, права и обязанности субъектов персональных данных)

5.2.1. Обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции РК, законов РК, иных нормативных правовых актов РК и реализации уставных задач Организации.

5.2.2. Принципы обработки персональных данных:

- законность целей и способов обработки персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Организации;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем, содержащих персональные данные.

5.2.3. Правовыми основаниями обработки персональных данных пациентов Организации выступают законодательство РК об охране здоровья граждан а также локальные нормативные акты Организации.

5.2.4. В отношениях по обработке персональных данных субъекты персональных данных имеют право:

а) получать полную информацию о своих персональных данных и об обработке этих данных (в том числе автоматизированной);

б) ознакамливаться со сведениями, содержащими свои персональные данные, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законом РК;

в) получать доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

г) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением закона РК; при отказе оператора исключить или исправить персональные данные субъект персональных данных имеет право заявить об этом в письменной форме администрации Организации.

5.2.5. При обращении субъекта персональных данных или его законного представителя по вопросам предоставления информации о персональных данных, относящихся к соответствующему субъекту, Организация обязана сообщить данному субъекту информацию о наличии персональных данных, предоставить возможность ознакомления с ней.

Обращения субъектов персональных данных фиксируются в журналах обращений по ознакомлению с персональными данными, которые ведутся в структурных подразделениях Организации по форме, утвержденной приказом главного врача Организации.

5.2.6. В отношениях, связанных с обработкой персональных данных, субъекты персональных данных обязаны:

а) передавать Организации достоверные персональные данные;

б) своевременно в срок, не превышающий 14 дней, сообщать Организации об изменении своих персональных данных.

5.3. Сроки обработки персональных данных

5.3.1. Общий срок обработки персональных данных определяется периодом времени, в течение которого Организация осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранение персональных данных.

5.3.2. Обработка персональных данных начинается с момента их получения Организацией и заканчивается:

- по достижении заранее заявленных целей обработки;
- по факту утраты необходимости в достижении заранее заявленных целей обработки.

5.3.3. Организация осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

5.4. Условия обработки персональных данных

5.4.1. Общим условием обработки персональных данных является наличие письменного согласия субъектов персональных данных на осуществление такой обработки.

Персональные данные Организация получает непосредственно от пациента.

Законами РК могут предусматриваться случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

5.4.2. Обработка персональных данных субъекта персональных данных без получения его согласия осуществляется в следующих случаях:
1) при поступлении официальных запросов (письменного запроса на бланке организации с печатью и росписью руководителя) из надзорно-контрольных или правоохранительных органов (суд, органы прокуратуры, МВД и т.п.);
2) при непосредственном обращении сотрудников правоохранительных или надзорно-контрольных органов при предъявлении ими служебного удостоверения и соответствующих документов о получении персональных данных (запрос, постановление и т.п.), а также в иных случаях, предусмотренных законом РК;
3) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
4) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
6) при обработке персональных данных, содержащихся в обращениях и запросах организаций и физических лиц;
7) обработка персональных данных осуществляется при регистрации и отправки корреспонденции почтовой связью.
5.4.3. Организация не имеет права получать и обрабатывать персональные данные пациента, в отношении религиозных и иных убеждений и частной жизни, а равно об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законом РК.
5.4.4. При принятии решений, затрагивающих интересы субъекта персональных данных, Организация не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
5.4.5. Обработка персональных данных осуществляется только должностными лицами (операторами) Организации, непосредственно использующими их в служебных целях (раздел 6 настоящего Положения).
Уполномоченные администрацией Организации на обработку персональных данных лица (операторы) имеют право получать только те персональные данные, которые необходимы для выполнения своих должностных обязанностей. Все остальные работники Организации имеют право на полную информацию, касающуюся только собственных персональных данных.
5.5. Уточнение, блокирование и уничтожение персональных данных
5.5.1. Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых Организацией.
5.5.2. Уточнение персональных данных осуществляется Организацией по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.
Об уточнении персональных данных Организация обязана уведомить субъекта персональных данных или его законного представителя.
5.5.3. Блокирование персональных данных осуществляется Организацией по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними.
О блокировании персональных данных Организация обязана уведомить субъект персональных данных или его законного представителя.
5.5.4. Уничтожение персональных данных осуществляется:

- по достижении цели обработки персональных данных;
- в случае утраты необходимости в достижении целей обработки персональных данных;
- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Организацией неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

5.5.5. В целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, Организация вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных.
О блокировании и (или) уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его законного представителя.

6. Доступ к персональным данным

6.1. Внутренний доступ (работники Организации)
6.1.1. Доступ к персональным данным пациентов имеют следующие должностные лица Организации, непосредственно использующие эти данные в рамках выполнения своих должностных обязанностей:

- главный врач;
- заместители главного врача по КЭР и медицинской работе;
- главный бухгалтер;
- руководители структурных подразделений;
- врачи и средний медицинский персонал, участвующие в оказании медицинских услуг пациенту;
- сотрудники юридического отдела.

6.1.2. Перечень работников Организации, имеющих в силу исполнения ими своих должностных обязанностей доступ к персональным данным, утверждается приказом главного врача Организации.
6.2. Условия обеспечения конфиденциальности информации
6.2.1. Должностные лица Организации, имеющие в силу исполнения ими своих должностных обязанностей доступ к персональным данным, при их обработке должны обеспечивать конфиденциальность этих данных.
Обеспечение конфиденциальности сведений, содержащих персональные данные, в Организации осуществляется в соответствии с «Инструкцией о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные», утвержденной главным врачом Организации и иными локальными нормативными актами.
6.2.2. Обеспечение конфиденциальности персональных данных не требуется:
1) в случае обезличивания персональных данных;
2) для общедоступных персональных данных, т.е. данных включенных в справочники, адресные книги и т.п.

6.3. Внешний доступ (другие организации и граждане)

6.3.1. Внешний доступ к персональным данным разрешается только при наличии заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с письменного согласия работника или пациента, персональные данные которого затребованы.
6.3.2. Сообщение сведений о персональных данных пациента его родственникам, членам семьи, иным близким ему людям также производится только при получении письменного согласия субъекта персональных данных.
6.3.3. Субъект персональных данных, о котором запрашиваются сведения, относящиеся к персональным данным, должен быть уведомлён о передаче его персональных данных третьим лицам.

6.3.4. Запрещается передача персональных данных в коммерческих целях без согласия субъекта персональных данных, а также иное использование персональных данных в неслужебных целях.

7. Защита персональных данных

7.1. Организация при обработке персональных данных принимает необходимые организационные и технические меры, в том числе использует шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

7.2. В целях обеспечения защиты персональных данных разрабатываются и утверждаются:

- планы мероприятий по защите персональных данных;
- планы внутренних проверок состояния защиты персональных данных;
- списки лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей;
- локальные нормативные акты и должностные инструкции;
- иные документы, регулирующие порядок обработки и обеспечения безопасности и конфиденциальности персональных данных.

7.3. Защита персональных данных от неправомерного их использования или утраты обеспечивается за счёт средств Организации в порядке, установленном законодательством РК.

7.4. В случае выявления неправомерных действий с персональными данными Организация обязана устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Организация обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его законного представителя.

7.5. Внутренняя защита персональных данных

7.5.1. Персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом несгораемом шкафу или в запираемом металлическом сейфе.

Выдача ключей от сейфа производится руководителем структурного подразделения, в функции которого входит обработка определенных персональных данных (а на период его временного отсутствия — болезнь, отпуск и т.п. — лицом, исполняющим ее обязанности), только сотрудникам данного структурного подразделения. Сдача ключа осуществляется лично руководителю после закрытия сейфа или несгораемого шкафа.

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

7.5.3. Персональные данные, содержащиеся на электронных носителях информации, хранятся в памяти персональных компьютеров операторов. Доступ к указанным персональным компьютерам строго ограничен кругом лиц, ответственных за обработку персональных данных.

Информация на электронных носителях должна быть защищена паролем доступа, который подлежит смене не реже 1 (одного) раза в 6 (шесть) месяцев.

7.5.4. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
и) анализ фактов не соблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
к) описание системы защиты персональных данных.
7.6. Внешняя защита персональных данных
7.6.1. Помещения и территория Организации охраняются, в том числе с помощью средств визуального наблюдения.
7.6.2. Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

8. Ответственность за разглашение персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законами РК.
8.2. Руководители структурных подразделений, в функции которых входит обработка персональных данных, несут персональную ответственность за нарушение порядка доступа работников данных структурных подразделений ТОО «Diamond Star» и третьих лиц к информации, содержащей персональные данные.
8.3. Должностные лица ТОО «Diamond Star» , обрабатывающие персональные данные, несут персональную ответственность за:
8.3.1) не обеспечение конфиденциальности информации, содержащей персональные данные;
8.3.2) неправомерный отказ субъекту персональных данных в предоставлении собранных в установленном порядке персональных данных либо предоставление неполной или заведомо ложной информации.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения главным врачом Организации и действует бессрочно, до замены его новым Положением.
9.2. Настоящее Положение действует в отношении всех работников.