УТВЕРЖДЕНО
приказом директора
Акционерного общества
«ДАНАЯ»
от «20» ноября 2024г № 73

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ И РАБОТНИКОВ АО «ДАНАЯ»

1. Общие положения.

1. Настоящим Положением об обработке и защите персональных данных определяется порядок обработки персональных данных пациентов (далее пациенты) и работников АО «ДАНАЯ» (далее Организация, Оператор).

2. Организация осуществляет обработку персональных данных пациентов и работников в целях обеспечения соблюдения законов и иных нормативных правовых актов, установления медицинского диагноза и оказания медицинских услуг.

3. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ №1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

4. Настоящее положение разработано в целях защиты персональных данных пациентов и работников Организации от несанкционированного доступа, неправомерного использования и утраты.

5. Настоящее Положение и изменения к нему утверждаются директором Организации и в соответствии с пунктом 2 статьи 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» подлежат опубликованию на сайте Организации.

6. Все сотрудники Организации, работающие с персональными данными пациентов, должны быть ознакомлены с настоящим Положением под роспись.

2. Основные понятия и состав персональных данных работников Организации.

2.1. В настоящем Положении в соответствии со статьей 3 Федерального закона от 27.07.2006г. N 152-ФЗ "О персональных данных" используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) 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;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.2. К персональным данным пациента или работника относится любая информация о нем, в том числе ФИО, дата рождения, адрес регистрации или проживания, семейное и социальное положение, должность, серия и номер паспорта, сведения о дате выдачи паспорта и выдавшем его органе , ИНН, СНИЛС, документы об образовании, номер амбулаторной карты, сведения о состоянии здоровья, в том числе группа здоровья, группа инвалидности и степень ограничения к трудовой деятельности, диагнозы по результатам обращения пациентов к врачу, информация об оказанных медицинских услугах, в том числе о проведенных лабораторных анализах и исследованиях и их результатах, выполненных оперативных вмешательствах и т.д.

Данные сведения являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

2.3. Персональные данные пациента содержатся в следующих документах:

- договоре на оказание платных медицинских услуг ;
- информированном добровольном согласии на оказание медицинских услуг ;
-медицинской карте пациента ;
- расходно-кассовых документах при оказании платных услуг;
- иных документах, в которых с учетом специфики деятельности Организации и в соответствии с законодательством РФ должны указываться персональные данные пациентов .

2.4. Персональные данные пациентов используются исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных 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.

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

2.6. Персональные данные работника работодатель получает непосредственно от работника. Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных в законодательстве.

2.7.При поступлении на работу работник заполняет заявление о приеме на работу, в котором указывает следующие

-сведения о себе:

– пол;
– дату рождения;
– семейное положение;
– отношение к воинской обязанности;
– местожительство и домашний телефон;
– образование, специальность;
– предыдущее(ие) место(а) работы;
– иные сведения, с которыми работник считает нужным ознакомить работодателя

2.8. Работодатель не вправе требовать от работника представления информации о политических и религиозных убеждениях и о его частной жизни.

2.9. Работник представляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

2.10. При изменении персональных данных работник письменно уведомляет работодателя о таких изменениях в разумный срок, не превышающий 14 дней.

2.11. По мере необходимости работодатель истребует у работника дополнительные сведения. Работник представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

2.12. Заявление о приеме на работу работника хранится в его личном деле. В личном деле также хранится вся информация, относящаяся к персональным данным работника. Ведение личных дел возложено на главного бухгалтера, ответственный за ведение личных дел главный бухгалтер организации.

3. Обработка персональных данных.

3.1. Обработка персональных данных пациентов или работников – это любое действие (операция) или совокупность действий (операций), совершаемых с использованием или без использования средств автоматизации, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.2. Перечень лиц, осуществляющих обработку персональных данных пациентов или работников либо имеющих к ним доступ, утверждается приказом директора.

3.3. Обработкой персональных данных пациента или работника без применения средств автоматизации является использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3.4. Сотрудники, осуществляющие обработку персональных данных пациентов без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных пациентов, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством РФ.

3.5. При фиксации персональных данных пациентов или работников на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.6. Если материальный носитель не позволяет осуществлять обработку персональных данных пациентов или работников отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных пациентов или работников 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;

- 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.

3.7. 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).

3.8. Уточнение персональных данных пациентов или работников 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.

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

3.10. Оператор обязан обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

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

3.12. В случае использования типовых форм, предполагающих или допускающих включение в них персональных данных, типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать: сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; фамилию, имя, отчество и адрес оператора; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения данных; сроки их обработки; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки персональных данных.

Типовая форма должна содержать поле, в котором субъект персональных данных может проставить отметку о согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения такого согласия.

3.13. Все персональные данные пациента следует получать у него самого. Пациент принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных даётся в письменной форме и должно быть конкретным, информированным и сознательным.

3.14. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, полномочия данного представителя на дачу согласия от субъекта персональных данных проверяются Оператором.

Согласие пациента на обработку его персональных данных должно храниться вместе с его иной медицинской документацией.

3.15. Письменное согласие пациента на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

3.16. Согласие на обработку персональных данных может быть отозвано пациентом или работников.

3.17. Персональные данные пациентов могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных".

3.18. При получении персональных данных не от пациента Организация до начала обработки таких персональных данных обязано предоставить пациенту следующую информацию:

наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные законодательством права субъекта персональных данных.

3.19. В случае недееспособности пациента согласие на обработку его персональных данных дает его законный представитель.

3.20. Оператор не имеет право получать и обрабатывать персональные данные пациента или работника о его политических, религиозных и иных убеждениях и частной жизни.

3.21. 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.

3.22. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается (на основании Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»):

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 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

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 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», 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 настоящим Федеральным законом.

4. Передача персональных данных пациентов и работников.

4.1. При передаче персональных данных пациентов или работников третьим лицам оператор должен соблюдать следующие требования:

4.1.1.Не сообщать персональные данные пациента или работника третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в других случаях, предусмотренных Федеральным законодательством РФ;

4.1.2. Предупредить лиц, получающих персональные данные пациента или 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.

Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности).

4.1.3. Разрешать доступ к персональным данным пациентов и работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

4.1.4. Передача персональных данных пациента сотрудникам оператора для выполнения должностных обязанностей должна осуществлять только в объёме, необходимом для выполнения их работы.

4.1.5. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности), в силу чего должны подписать обязательство о неразглашении конфиденциальной информации..

4.2. Согласие пациента на передачу персональных данных не требуется, если законодательством РФ установлена обязанность предоставления оператором персональных данных (пункты 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", статьи 13 Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ»).

4.3. **Трансграничная передача данных в Организации не производится.**

5. Доступ к персональным данным пациентов и работников.

5.1. Право доступа к персональным данным пациентов (доступ внутри Организации) имеют:

- директор Организации
- главный врач Организации
- лечащие врачи Организации
- медицинские сестры Организации.

Лица, имеющие право доступа к персональным данным пациентов назначаются приказом директора Организации.

5.2. Указанные в пункте 5.1. лица имеют право получать только те персональные данные пациентов, которые необходимы им для выполнения своих должностных обязанностей.

5.3. Персональные данные вне Организации могут представляться в государственные и негосударственные функциональные структуры (внешний доступ):

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в государственные органы, в объеме, предусмотренном законом;
- в налоговые органы;
- в военные комиссариаты;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом

5.4. Персональные данные пациента третьей стороне могут быть предоставлены только с письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента.

5.5. Персональные данные пациента могут быть предоставлены его законному представителю, а также родственникам или членам его семьи, иным представителям только с письменного разрешения самого пациента либо его законного представителя.

5.6. В целях обеспечения защиты персональных данных, хранящихся в Организации, пациенты имеют право:

5.6.1. На получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства РФ;

5) обрабатываемые персональные данные, относящиеся к соответствующему пациенту, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством РФ;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) иные сведения, предусмотренные федеральным законодательством РФ, за исключением случаев, предусмотренных ч. 8 ст.14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Вышеуказанные сведения должны быть предоставлены пациенту оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5.6.2. Пациент вправе требовать от оператора 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.

5.6.3. Сведения, указанные в п.5.6.1. ст.5.6. настоящего Положения, предоставляются пациенту или его представителю оператором при обращении либо при получении запроса пациента или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность пациента или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие пациента в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись пациента или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.6.4. В случае, если сведения, указанные в п. 5.6.1. ст.5.6. настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления пациенту по его запросу, пациент вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 5.6.1. ст.5.6. настоящего Положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством или договором, стороной которого является пациент.

5.6.5. Пациент вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных п.5.6.1. ст.5.6 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п.5.6.1. ст.5.6. настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п.5.6.1. ст.5.6. настоящего Положения, должен содержать обоснование направления повторного запроса.

5.6.6. Оператор вправе отказать пациенту в выполнении повторного запроса, не соответствующего условиям, предусмотренным п.5.6.1., 5.6.5. ст.5.6. настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

5.6.7. Решение, порождающее юридические последствия в отношении пациента или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме пациента или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов пациентов.

Оператор обязан разъяснить пациенту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты пациентом своих прав и законных интересов. Оператор обязан рассмотреть указанное возражение в течение тридцати дней со дня его получения и уведомить пациента о результатах рассмотрения такого возражения.

5.6.8. Если пациент считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Положения или иным образом нарушает его права и свободы, пациент вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных, также пациент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, в судебном порядке.

5.7. Доступ к персональным данным работников АО «ДАНАЯ», не требующий подтверждения и не подлежащий ограничению, имеют:

- заместитель директора АО «ДАНАЯ»;
- главный бухгалтер АО «ДАНАЯ».

5.8. Доступ к персональным данным работников АО «ДАНАЯ» для иных лиц

может быть разрешен только отдельным распоряжением директора.

6.Защита и хранение персональных данных пациентов и работников.

6.1. При обработке персональных данных пациентов и работников Организация обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

6.2. Защите подлежит:

- информация о персональных данных пациента и работника;
- документы, содержащие персональные данные пациента и работника ;
- персональные данные пациентов и работников, содержащиеся на электронных носителях.

6.3. В соответствии с требованиями статьи 22.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» приказом директора Организации назначается лицо, ответственное за организацию обработки персональных данных.

6.5. Лица, осуществляющие обработку персональных данных и/или, имеющие доступ к персональным данным обязаны подписать письменное обязательство о соблюдении конфиденциальности персональных данных пациентов и соблюдении правил их обработки.

6.6. Лица, осуществляющие обработку персональных данных и/или, имеющие доступ к персональным данным пациентов обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации, в том числе:

- соблюдать режим секретности (конфиденциальности) ;
- немедленно информировать директора о фактах нарушения режима конфиденциальности информации, о попытках других лиц получить (узнать) конфиденциальную информацию о персональных данных, или о попытках несанкционированного доступа к информационным ресурсам с целью получения таких сведений; об утрате или недостаче носителей, содержащих конфиденциальную информацию и документов, содержащих конфиденциальную информацию, ключей от помещений, металлических шкафов и печатей, а также обо всех других случаях, которые могут повлечь за собой разглашение информации о персональных данных.

6.7. Лицу, работающему с персональными данными, запрещается:

- разглашать информацию о персональных данных в любой форме (устной, письменной или электронной);
- оставлять документы и иные носители, содержащие персональные данные в незакрытом помещении, в котором хранятся персональные данные пациентов;
- допускать ознакомление с документами и иными носителями, содержащими персональные данные пациентов, других сотрудников, не имеющих право доступа к персональным данным;

- передавать сведения о персональных данных в устной форме, по телефону, на бумажных и машинных носителях, в электронной форме и т.д. другим лицам, не имеющим доступа к этим сведениям;

- использовать информацию, содержащую персональные данные пациентов и работников в открытой переписке, статьях и выступлениях, а также в личных интересах;

- копировать для личного использования, будучи сотрудником Организации или при увольнении документы, содержащие персональные данные пациентов и работников.

6.8. Для обеспечения защиты персональных данных директор:

6.8.1. Утверждает приказом состав работников, функциональные обязанности которых требуют доступа к персональным данным пациентов и работников.

6.8.2. Обеспечивает раздельное хранение материальных данных (материальных носителей), обработка которых осуществляется в различных целях.

6.8.3. В помещениях, в которых ведется работа с персональными данными, обеспечена сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6.8.4. Материальные носители персональных данных пациентов и работников Организации хранятся в отдельном кабинете, закрывающемся на ключ.

6.8.5. Доступ к информации в электронном виде осуществляется с использованием парольной защиты, а в информационных системах персональных данных - с использованием средств автоматизации в соответствии с нормативными документами.

Защита сведений с персональными данными, хранящимися в электронных базах данных от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей:

- для каждого работника, работающего с персональными данными, заводится отдельная учетная запись для входа в компьютер;

- до начала работы работник должен ввести свое имя и пароль, при этом пароль не должен быть виден на экране;

- после нескольких неправильных попыток ввода пароля учетная запись пользователя блокируется;

- если пользователь бездействует на протяжении нескольких минут, вход в систему закрывается.

6.8.6. Обеспечение безопасности персональных данных в информационных системах персональных данных осуществляется в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 N 1119.

6.8.7. Выбор и реализация методов и способов зашиты информации в информационной системе осуществляется на основе определяемых Организацией угроз безопасности персональных данных (модели угроз) и в зависимости от уровня защищенности информационной системы, определенного в соответствии с «Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 N 1119.

6.8.9. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных.

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

7.1. За неисполнение или ненадлежащее исполнение работником Организации или по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными пациентов работник Организации может быть привлечен к дисциплинарной, материальной, административной и уголовной ответственности в порядке, установленном федеральным законом.

7.2. 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 РФ об административных правонарушениях.