ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ и ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ПАЦИЕНТОВ ООО «Снежок»

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных пациентов ООО «Снежок» (далее – Медицинский центр) от несанкционированного доступа.

1.2. Настоящее Положение разработано в соответствии с требованиями ТК РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федерального закона РФ от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и определяет особенности обработки персональных данных пациента.

1.3. Сбор, хранение, использование и распространение информации о состоянии здоровья пациента без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.4. Лица, в обязанность которых входит ведение персональных данных пациентов, обязаны обеспечить возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.6. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

1.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов согласно законодательства Российской Федерации.

1.9. Настоящее Положение утверждается генеральным директором Медицинского центра и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным пациента.

2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ПОЛОЖЕНИИ

2.1. Для целей настоящего Положения в тексте применяются следующие термины и определения:

- **Врачебная тайна** – соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении;
- **Персональные данные пациента** - 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, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность, номер амбулаторной карты, номер истории болезни, сведения о состоянии здоровья, в том числе группа здоровья, группа инвалидности и степень ограничения к трудовой деятельности, состояние диспансерного учета, зарегистрированные диагнозы по результатам обращения пациентов к врачу, в том числе при прохождении диспансеризации и медицинских осмотров, информация об оказанных медицинских услугах, в том числе о проведенных лабораторных анализах и исследованиях и их результатах, выполненных оперативных вмешательствах, случаях стационарного лечения их результатах, о выданных листах временной нетрудоспособности с указанием номера листа нетрудоспособности и периода нетрудоспособности, регистрация прикрепления на территории обслуживания пациента – дата и признак прикрепления, информация о выписанных и отпущенных лекарственных средствах и изделиях медицинского назначения, информация о наличии льгот (по категориям), о документах, подтверждающих право на льготу и право на льготное лекарственное обеспечение, дата и причина смерти гражданина в случае его смерти;

- **Документы (носители), содержащие персональные сведения пациента** – формы медицинской и иной учетно-отчетной документации, включающие сведения о персональных данных.

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

- **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 затрагивающих 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;

- **Конфиденциальность персональных данных** - обязательное для соблюдения Учреждением-оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

- **Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

- **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.

3. Права и обязанности пациента

3.1. Пациент имеет право:

- получения полной информации о своих персональных данных и обработке персональных данных, состоянии и прогнозе своего здоровья;
- доступа к своим медицинским данным с помощью специалиста, ответственного за ведение данных;
- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований и настоящего Положения;
- заявить в письменной форме о своем несогласии с соответствующим обоснованием такого;
- свободного бесплатного доступа к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определять своих представителей для защиты своих персональных данных.

3.1. Пациент обязан:

- 3.1.1. Передавать лицу, обрабатывающему персональные данные, комплекс достоверных, документированных персональных данных, информацию о состоянии здоровья.
- 3.1.2. Своевременно сообщать лицу, использующему персональные данные пациента, об их изменениях.

3.2. Пациент не должен отказываться от своих прав на сохранение и защиту тайны.

4. Перечень документов и сведений, содержащих персональные данные пациента

4.1. В соответствии с Федеральным законом РФ от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», локальными нормативными актами Медицинского центра, лицо, обратившиеся, предъявляет регистраторам следующие документы, содержащие его персональные данные:

- паспорт или иной документ, удостоверяющий личность, содержащий сведения о месте регистрации (месте жительства), сведения о семейном положении;
- страховое свидетельство фонда ОМС, страховой компании, содержащее сведения о номере и серии страхового свидетельства.

4.2. В перечень документов и сведений, содержащих персональные данные, включаются:

- сведения о состоянии здоровья;

- анкетные и паспортные данные;
- семейное положение;
- другая информация.

5. Требования по обработке персональных данных пациентов. Сбор, обработка и хранение персональных данных

5.1. В целях обеспечения прав и свобод человека и гражданина лица, участвующие в обработке персональных данных пациента, обязаны соблюдать следующие общие требования:

- обработка персональных данных пациента может осуществляться лицами имеющими допуск исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, контроля количества и качества выполняемой работы;
- при определении объема и содержания обрабатываемых персональных данных пациента лица, участвующие в процессе обработки, должны руководствоваться Конституцией РФ, Федеральным законом РФ от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иными федеральными законами;
- все персональные данные пациента следует получать у него самого или у его представителя.

5.2. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

5.3.Работник Медицинского центра должен сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

5.4. Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Медицинским центром за счет своих средств в порядке, установленном федеральным законом.

5.5. Пациенты и их представители должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных пациента, а также об их правах и обязанностях в этой области.

5.6. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным при сборе персональных данных;
- достоверности персональных данных и их достаточности;
- личной ответственности сотрудников медицинского центра за сохранность и конфиденциальность персональных данных, а также носителей этой информации
- наличие четкой разрешительной системы доступа сотрудников Медицинского центра к документам и базам данных, содержащим персональные данные.

5.7. Порядок получения персональных данных:

Получение персональных данных преимущественно осуществляется путем представления их пациентом, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством РФ.

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

- фамилию, имя, отчество, адрес пациента - 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 Медицинского центра, получающего согласие пациента - 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 Медицинским центром способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Для обработки персональных данных, содержащихся в согласии в письменной форме пациента на обработку его персональных данных, дополнительное согласие не требуется.

5.8. Обработка, передача и хранение персональных данных пациента:

5.8.1. Все действия по обработке персональных данных пациента осуществляются только работниками Медицинского центра, допущенными приказом генерального директора к работе с персональными данными пациента, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

5.9. Этапность получения и обработки персональных данных пациента.

5.9.1. При первичном посещении медицинского центра пациентом информация заносится в базу данных в регистратуре. На этом этапе регистратор отмечает паспортные данные, контактный телефон, место работы и должность, Ф.И.О специалиста к которому желает попасть пациент. Оформляется амбулаторная карта, которая является основным документом, содержащим персональные данные пациента, в которой фиксируются выше перечисленные персональные данные. Информация о пациенте хранится как на электронном, так и на бумажном носителе информации о персональных данных. Регистратор не вправе получать информацию о состоянии здоровья пациента. Ответственным на данном этапе хранения персональных данных является регистратор, фиксирующий персональные данные.

5.9.2. Амбулаторная карта передается врачу. Врач собирает информацию о состоянии здоровья пациента, фиксирует в амбулаторную карту. Ответственным за неразглашения информации о состоянии здоровья является врач. При передаче персональных данных пациента врач должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные пациента, 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). Данное положение не распространяется на обмен персональными данными пациента в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным пациента только специально уполномоченным лицам, при этом указанные лица должны иметь право

получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций.

5.9.3. По окончании приема медицинская карта сдается врачом-специалистом в регистратуру Медицинского центра.

5.9.4. После получения медицинских услуг носитель, содержащий персональные данные о состоянии здоровья, диагнозе, проведенном лечении и рекомендациях хранится в регистратуре медицинского центра.

5.10. Все меры конфиденциальности при сборе, обработке и хранении персональных данных пациента распространяются на бумажные носители.

5.11. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

5.12. С работниками, ответственными за хранение персональных данных, а также с работниками, владеющими персональными данными в силу своих должностных обязанностей, заключаются Соглашения о неразглашении персональных данных пациентов. Экземпляр Соглашения хранится в отделе кадров. В должностные инструкции данных работников включается пункт об обязанности сохранения врачебной тайны.

5.13. Автоматизированная обработка и хранение персональных данных пациентов допускаются только после выполнения всех основных мероприятий по защите информации.

5.14. Журналы и другие формы медицинской документации, находящиеся в обработке и содержащие персональные данные пациентов, оформляются и хранятся в подразделениях медицинского центра в соответствии с требованиями действующих локальных приказов.

Прочие документы, используемые при оказании медицинской помощи и содержащие персональные данные пациентов (акты, направления, договоры, квитанции и пр.), после оформления передаются работнику, допущенному к работе с персональными данными, в должностные обязанности которого входит обработка этих данных.

Хранение оконченных производством документов, содержащих персональные данные пациентов, осуществляется в архиве медицинского центра.

5.15. Проведение уборки помещения должно производиться в присутствии ответственного лица.

5.16. Регламент работы с медицинской документацией утверждён приказом Медицинского центра.

6. Доступ к персональным данным пациента

6.1. Доступ к персональным данным физического лица имеют должностные лица, непосредственно использующие их в служебных целях.

6.2. Уполномоченные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

6.3. Сведения о пациенте могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления пациента.

6.4. Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

ТРЕТЬИМ ЛИЦАМ

7.1. Передача персональных данных пациентов третьим лицам осуществляется Медицинским центром только с письменного согласия пациента, с подтверждающей визой генерального директора, за исключением случаев, предусмотренных ст. 13 Федерального закона РФ от 21 ноября 2011 г. N 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 учётом положений пункта 1 части 9 статьи 20 указанного Федерального закона;

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 указанного Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 указанного Федерального закона, 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 причинён 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 указанным Федеральным законом.

Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками несут ответственность за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

7.2. Медицинский центр обеспечивает ведение журнала учета выданных персональных данных пациентов, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных пациента, либо отсутствует письменное согласие

пациента на предоставление его персональных данных, Медицинский центр обязан отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдаётся в мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится в Медицинском центре.

8. Защита персональных данных

8.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа,
- реализацию права на доступ к информации.

8.2. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании.

8.3. Для защиты персональных данных пациента необходимо соблюдать ряд мер:

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава лиц, имеющих право доступа (входа) в помещение, в котором находятся персональные данные пациента

- организация порядка уничтожения информации;

- своевременное выявление нарушений требований разрешительной системы доступа;

- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

8.4. Бумажные носители информации могут выдаваться на рабочие места, только работникам Медицинского центра, допущенным приказом генерального директора к работе с персональными данными пациента.

8.5. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

8.6. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности медицинского центра, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения источников информации о состоянии здоровья пациента.

8.7. Для защиты персональных данных пациентов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при опросе и сборе анамнеза.

8.8. Для обеспечения безопасности персональных данных пациента при неавтоматизированной обработке предпринимаются следующие меры:

8.8.1. Все действия по обработке персональных данных работника осуществляются только работниками Медицинского центра, допущенными приказом главного врача к работе с персональными данными пациента, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

8.8.2. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

8.9. Для обеспечения безопасности персональных данных пациентов при автоматизированной обработке предпринимаются следующие меры:

8.9.1.Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 01.11. 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8.10. Хранение персональных данных пациентов осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные пациентов, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению в порядке, предусмотренном приказами по архивному делу.

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

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

9.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.2. Каждый сотрудник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут в соответствии с федеральными законами ответственность:

- дисциплинарную (замечание, выговор, увольнение);
- административную (предупреждение или административный штраф);
- гражданско-правовую (возмещение причиненного убытка).

10. Заключительные положения

10.1. Настоящее Положение вступает в силу с момента его утверждения директором и вводится в действие приказом генерального директора Медицинского центра.

10.2. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании приказа генерального директора Медицинского центра.

10.3. Настоящее Положение распространяется на всех пациентов, обращающихся за медицинской помощью в Медицинский центр, а так же сотрудников Медицинского центра, имеющих доступ и осуществляющих перечень действий с персональными данными пациентов.

10.4. В обязанности работников осуществляющих первичный сбор персональных данных пациента входит их информирование о возможности ознакомление с настоящим положением, и обязательное получение согласия пациента на обработку его персональных данных.