Политика безопасности в отношении обработки персональных данных, сведения о реализуемых требованиях к защите персональных данных

# 1. Термины и определения

 Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

 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.

 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.

 Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

 Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

 Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

 Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

 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.

 Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

 Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

# 2. Назначение и правовая основа документа

 Политика ООО «Дипломат» (далее по тексту – Клиника) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Клиника в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

 Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

 Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных организации позволит оптимизировать затраты на ее построение.

 При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

 Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

# 3. Основными объектами системы безопасности персональных данных Клинике являются:

* - информационные ресурсы с ограниченным доступом, содержащие персональные данные;
* - процессы обработки персональных данных в информационных системах персональных данных Клиники, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
* - информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

# 4. Интересы затрагиваемых субъектов информационных отношений

 Субъектами информационных отношений при обеспечении безопасности персональных данных Клиники являются:

* - Клиника, как собственник информационных ресурсов;
* - руководство и работники Клиники, в соответствии с возложенными на них функциями;
* - физические лица, не являющиеся сотрудниками Клиники, но имеющими с ней отношения.
* Перечисленные субъекты информационных отношений заинтересованы в обеспечении:
* - своевременного доступа к необходимым им персональным данным (их доступности);
* - достоверности (полноты, точности, адекватности, целостности) персональных данных;
* - конфиденциальности (сохранения в тайне) персональных данных;
* - защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
* - разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
* - возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
* - защиты персональных данных от незаконного распространения.

## 4.1. Цели защиты

 Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Клиники от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

 Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

* - доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Клиники, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
* - целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Клиники и передаваемой по каналам связи;
* - конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

 Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

## 4.2. Основные задачи системы обеспечения безопасности персональных данных

 Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Клиники должна обеспечивать эффективное решение следующих задач:

* - своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Клиники;
* - создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
* - создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
* - защиту от вмешательства в процесс функционирования информационных систем Клиники посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Клиники (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
* обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* защиту от несанкционированной модификации используемых в информационных системах Клиники программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
* защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

## 4.3. Основные пути решения задач системы защиты

 Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

* - строгим учетом всех подлежащих защите ресурсов информационных систем Клиники (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
* - фиксацией действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;
* - полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Клиники по вопросам обеспечения безопасности информации;
* - подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
* - наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Клиники;
* - четким знанием и строгим соблюдением всеми пользователями информационных систем Клиники, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
* - персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Клиники;
* - непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Клиники;
* - применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
* - эффективным контролем над соблюдением пользователями информационных ресурсов Клиники требований по обеспечению безопасности информации;
* - юридической защитой интересов Клиники при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

# 5. Построение системы, обеспечения безопасности персональных данных Клиники, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

* - законность;
* - системность;
* - комплексность;
* - непрерывность;
* - своевременность;
* - преемственность и непрерывность совершенствования;
* - разумная достаточность (экономическая целесообразность);
* - персональная ответственность;
* - минимизация полномочий;
* - исключение конфликта интересов;
* - взаимодействие и сотрудничество;
* - гибкость системы защиты;
* - открытость алгоритмов и механизмов защиты;
* - простота применения средств защиты;
* - обоснованность и техническая реализуемость;
* - специализация и профессионализм;
* - обязательность контроля.

# 6. Меры обеспечения информационной безопасности

 Все меры обеспечения безопасности информационных систем Клиники подразделяются на:

* - правовые (законодательные);
* - морально-этические;
* - технологические;
* - организационные (административные);
* - физические;
* - технические (аппаратурные и программные).

# 7. Отзыв согласия на обработку ПДн субъектов (пациенты)

 В соответствии со ст.3 ФЗ «О персональных данных» (Далее по тексту-Закон) персональными данными (далее по тексту-ПД) является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД). Любые действия (операции) с ПД, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу) обезличивание, блокирование, уничтожение ПД признаются обработкой ПД.

 Обработка ПД допускается только с согласия субъектов ПД, за исключением случаев, перечисленных в п.п. 2-11 части 1 ст.6 Закона.

 Вместе с тем, в силу части 2 статьи 6 Закона обработка отдельных категорий ПД в том числе сведений касающихся состояния здоровья, регулируются специальными правилами ст. 10 Закона. Подобные сведения могут обрабатываться без согласия субъектов ПД в случаях, предусмотренных п.п. 2-9 части 2 статьи 10 Закона. К таковым случаям относятся, в частности персональные данные, обработка которых, осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

 В соответствии со статьей 13 ФЗ Об основах охраны здоровья граждан в Российской Федерации» 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.

 В соответствии с частью 2 статьи 13 ФЗ «Об основах охраны здоровья граждан в Российской Федерации», не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицам, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 настоящей статьи.

 Таким образом, режим врачебной тайны, распространяется не только на медицинский персонал, но и на иных лиц состоящих в трудовых отношениях с медицинской организацией.

 Однако, согласно п.4 части 10 Закона обработка ПД без согласия субъекта ПД в медицинских целях допускается только лицом, профессионально осуществляющим медицинскую деятельность.

 В соответствии с частью 2 ст. 9 Закона субъект ПДн вправе отозвать свое согласие на их обработку.

 Согласно ч. 5, ч. 6 ст. 21 Закона в случае отзыва субъектом ПД согласия на обработку его ПД оператор обязан прекратить их обработку и уничтожить их, если их сохранение более не требуется для целей обработки ПД. Для этого оператору предоставляется срок, не превышающий тридцати дней, с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом ПД либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных данным законом или другими федеральными законами. При отсутствии возможности уничтожить ПД в 30-дневный срок оператор должен их блокировать и обеспечить их уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

 Между тем, информация о состоянии здоровья отдельного гражданина фиксируемая в его медицинской карте, имеет огромное значение, как для самого гражданина, так и для неопределенного круга лиц, в первом случае - для установления клинической картины гражданина, во втором случае - для определения угроз возникновения эпидемий и социально-значимых заболеваний. В этих целях согласно пункту 12. ч.1 ст.79 Закона о «Об охране здоровья граждан в Российской Федерации», медицинские организации обязаны обеспечивать учет и хранение медицинской документации, а приказом Минздрава СССР от 04.10.1980 года №1030 утверждены сроки хранения первичной медицинской документации учреждений здравоохранения, где для хранения амбулаторных медицинских карт установлен срок хранения 25 лет.

 На основании изложенного, во исполнение требований ФЗ «О персональных данных» ФЗ «Об охране здоровья граждан Российской Федерации» в ООО «Дипломат» устанавливается следующий порядок действий в случае отзыва субъектом персональных данных согласия на обработку персональных данных.

 Отзыв на обработку ПД оформляется в письменном виде, по установленной форме. С момента получения отзыва, прекращается обработка субъекта ПД с использованием средств автоматизации.

 Отзыв передается в администрацию клиники для уничтожения ПД содержащихся в системе автоматизации в течении 30 дней с момента получения соответствующего отзыва. Уничтожение ПД субъекта оформляется актом, один экземпляр которого совместно с отзывом на обработку ПД передается в регистратуру для приобщения к медицинской карте.

 Медицинская карта субъекта ПД передается в установленном порядке в архив ООО «Дипломат» на хранение.

# 8. Отзыв согласия на обработку ПДн субъектов (работники)

 В случае, если работник Клиники при увольнение отзывает ранее данное согласие на обработку персональных данных следует учитывать следующие положения Закона.

 В силу п. 2 ч. 1 ст. 6 Закона «О персональных данных» обработка персональных данных без согласия субъектов персональных данных допускается если:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

 В соответствии со статьей 15 ФЗ «О страховых взносах в Пенсионный фонд РФ, Фонд социального страхования РФ, Федеральный фонд обязательного медицинского страхования, ООО «Дипломат», являясь работодателем, и выступая в качестве плательщика страховых взносов, обязана предоставлять в территориальные органы Пенсионного фонда РФ и Фонда социального страхования РФ отчетность.

 Соответственно, направляя документы, содержащие персональные данные уволенного работника в указанные фонды, ООО «Дипломат» выступая в качестве работодателя, будет выполнять обязанность, возложенную на нее федеральным законодательством, поэтому получать согласие работника на обработку персональных данных в таком случае не нужно.

 Согласно ч. 5, ч. 6 ст. 21 Закона «О персональных данных», в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и уничтожить их, если их сохранение более не требуется для целей обработки персональных данных.

 Согласно пункту 1 статьи 17 Закона об архивном деле, государственные органы, органы местного самоуправления, организации и граждане, занимающиеся предпринимательской деятельностью без образования юридического лица, обязаны обеспечивать сохранность архивных документов, в том числе документов по личному составу, в течение сроков их хранения, установленных федеральными законами, иными нормативными правовыми актами Российской Федерации, а также перечнями документов, предусмотренными частью 3 статьи 6 и частью 1 статьи 23 настоящего Федерального закона.

 Пунктом 8 статьи 23 Налогового кодекса Российской Федерации установлена обязанность налогоплательщика в течение четырех лет обеспечивать сохранность данных бухгалтерского и налогового учета и других документов, необходимых для исчисления и уплаты налогов, в том числе документов, подтверждающих получение доходов, осуществление расходов (для организаций и индивидуальных предпринимателей), а также уплату (удержание) налогов.

 Статья 17 Федерального закона от 21.11.1996 N 129-ФЗ "О бухгалтерском учете" возлагает на организации обязанности по хранению первичных учетных документов, регистров бухгалтерского учета и бухгалтерской отчетности в течение сроков, устанавливаемых в соответствии с правилами организации государственного архивного дела, но не менее пяти лет; рабочего плана счетов бухгалтерского учета, других документов учетной политики, процедуры кодирования, программной машинной обработки данных (с указанием сроков их использования) не менее пяти лет после года, в котором они использовались для составления бухгалтерской отчетности в последний раз.

 Часть 2 ст. 9 Закона N 152-ФЗ специально оговаривает, что оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных в случае отзыва им согласия на их обработку при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 данного закона.

 Исходя из вышеизложенного следует признать, что к таковым относятся случаи обработки персональных данных без согласия работника.

 Таким образом, в случае отзыва работником согласия на обработку его персональных данных, прекращается их обработка и уничтожается за исключением тех данных, которые могут обрабатываться без согласия работника, в том числе:

* - сведения о работнике, направляемые в ПФР и ФСС;
* - сведения, по личному составу содержащиеся в управленческих архивных документах в порядке определенном приказом Министерства культуры РФ от 25.08.2010 г. №558