УТВЕРЖДАЮ
Главный врач
ГБУ РО «СП № 1» в г. Ростове-на-Дону

_____ Задорожний А.В.
«__» _____ 2025 г.
М.П.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБРАБОТКЕ И ЗАЩИТЕ ПДН, ОБРАБАТЫВАЕМЫХ В ИСПДН

1. Общие положения

1.1 Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных в государственные бюджетные учреждения Ростовской области «Стоматологическая поликлиника № 1» в г. Ростове-на-Дону (далее – учреждение) и при их обработке в ИСПДн медицинской информационной системе персональных данных «ВебМИС» государственного бюджетного учреждения Ростовской области «Стоматологическая поликлиника № 1» в г. Ростове-на-Дону (далее – ИСПДн).

Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных"; Постановлений Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и других нормативных правовых актов Российской Федерации, а также порядок обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы).

1.2 В части защиты информации настоящее Положение разработано с учетом требований Постановления Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Положение не распространяется на отношения, связанные с обеспечением безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.3 В настоящем Положении используются следующие основные понятия:

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, другая информация;

обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), 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 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;

неавтоматизированная обработка персональных данных, содержащихся в информационной системе, либо извлеченных из такой системы (без использования средств автоматизации), – обработка, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

конфиденциальность персональных данных – обязательное для соблюдения получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных, при их обработке в информационной системе 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;

технические средства обработки персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах персональных данных;

персональные данные гражданского служащего – сведения о фактах, событиях и обстоятельствах жизни гражданского служащего Российской Федерации, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего, либо подлежащие включению в его личное дело;

ответственное должностное лицо – работник учреждения, который приказом руководителя учреждения допущен к обработке персональных данных.

1.4 Представитель нанимателя в лице работника кадрового подразделения государственного бюджетного учреждения Ростовской области "Стоматологическая поликлиника № 1» в г. Ростове-на-Дону обеспечивает защиту персональных данных работников учреждения, переданных в кадровый отдел учреждения, от неправомерного их использования или утраты.

1.5 Руководитель учреждения определяет лиц из числа работников учреждения, обеспечивающих обработку персональных данных (далее – уполномоченные работники) в соответствии с требованиями нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

1.6 Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации а также порядок обезличивания ПДн.

2. Требования к обработке персональных данных

2.1. При обработке персональных данных уполномоченные работники обязаны соблюдать следующие требования:

а) обработка персональных данных осуществляется в целях обеспечения соблюдения

Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия субъекту персональных данных в реализации его прав в пределах полномочий учреждения;

б) персональные данные могут быть получены у субъекта персональных данных как лично, так и у третьей стороны любым законным путем при соблюдении условия, изложенного в подпункте «а» настоящего пункта;

в) запрещается получать и обрабатывать не установленные Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" персональные данные, а также персональные данные, получение которых не связано с деятельностью учреждения;

г) при принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

д) защита персональных данных субъекта персональных данных от неправомерного их использования или утраты обеспечивается за счет средств учреждения в порядке, установленном Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и иными нормативными правовыми актами Российской Федерации;

е) передача персональных данных субъекта персональных данных третьей стороне не допускается без его письменного согласия, за исключением случаев, установленных федеральными законами;

ж) учреждением обеспечивается конфиденциальность обрабатываемых персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

з) в случае выявления недостоверных персональных данных субъекта персональных данных или неправомерных действий с ними ответственных лиц при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, осуществляется блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки;

и) в случае подтверждения факта недостоверности персональных данных субъекта персональных данных, на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, персональные данные уточняются и осуществляется их разблокирование;

к) в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, допущенные нарушения устраняются. В случае невозможности устранения допущенных нарушений, в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, персональные данные уничтожаются. Об устранении допущенных нарушений или об уничтожении персональных данных субъект персональных данных или его законный представитель уведомляются, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также и указанный орган;

л) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели их обработки, а персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

2.2. В целях обеспечения защиты персональных данных, переданных непосредственно учреждению, субъекты персональных данных имеют право:

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

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

в) требовать исключения или исправления неверных или неполных персональных данных. Субъект персональных данных при отказе уполномоченного работника исключить или исправить его персональные данные имеет право заявить в письменной форме руководителю учреждения о своем несогласии, обосновав такое несогласие соответствующим образом.

г) требовать от уполномоченных работников учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;

д) обжаловать действия или бездействие уполномоченных работников в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных, считает, что обработка его персональных данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" или иным образом нарушает его права и свободы.

2.3. Уполномоченный работник, виновный в нарушении норм, регулирующих получение, обработку, хранение и передачу персональных данных, несет ответственность в соответствии с федеральными законами.

3. Мероприятия по обеспечению безопасности персональных данных

3.1. Мероприятия по обеспечению безопасности персональных данных включают в себя:

а) сбор сведений о наличии в учреждении информационных систем персональных данных и документов, содержащих персональные данные;

б) формирование списка документов, содержащих персональные данные, списка информационных систем персональных данных учреждения, списка ответственных должностных лиц, списка помещений в которых производится обработка персональных данных.

Указанные списки утверждаются приказом руководителя учреждения. Приказ доводится до ответственных должностных лиц установленным в учреждении порядком;

в) учет ответственных должностных лиц, допущенных к работе с персональными данными;

г) в случае поручения учреждением на основании договора обработки персональных данных другому лицу (далее – уполномоченное лицо), отражение в договоре обязанности обеспечения указанным лицом конфиденциальности персональных данных;

д) учет передачи персональных данных третьим лицам, в т.ч. уполномоченным лицам, ответственным представителям уполномоченных лиц.

3.2. Конфиденциальность персональных данных при их обработке без использования средств автоматизации обеспечивают ответственные должностные лица и/или уполномоченные лица.

3.3. Безопасность персональных данных при их обработке в информационных системах персональных данных учреждения обеспечивают ответственные должностные лица и/или уполномоченные лица. В договоре с уполномоченным лицом необходимо предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в указанных информационных системах либо отбирать соответствующее обязательство.

3.4. Повседневный контроль за соблюдением требований по защите персональных данных осуществляется начальниками структурных подразделений, в которых ведется обработка персональных данных.

Подразделение по защите информации учреждения осуществляет методическую помощь в построении подсистем защиты персональных данных и общий контроль за соблюдением требований по защите персональных данных в информационных системах персональных данных учреждения.

3.5. Лица, виновные в нарушении требований законодательства Российской Федерации в области защиты персональных данных, несут, гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

3.6 Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем учреждения, и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем учреждения назначается администратор информационной безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

4. Организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

4.1. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах персональных данных учреждения обеспечивается в рамках единой системы защиты информации, а также подсистем защиты персональных данных указанных информационных систем. Подсистемы защиты персональных данных включают организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных).

4.2. Возможные каналы утечки информации при обработке персональных данных, методы и способы защиты информации в информационных системах персональных данных определяются и разрабатываются с использованием руководящих документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

4.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных являются составной частью работ по созданию информационных систем персональных данных.

В случае, если учреждение на основании договора поручает создание информационной системы персональных данных другому лицу, в договоре отражается обязанность обеспечения указанным лицом безопасности персональных данных.

4.5. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в информационных системах персональных данных, должны пройти в установленном порядке процедуру оценки соответствия (сертификацию).

4.6. Информационные системы персональных данных учреждения классифицируются постоянно действующей технической комиссией по контролю защищенности ПДн.

4.7. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации достаточных организационных мер и/или путем применения технических средств.

Организационные меры и/или технические средства определяются и разрабатываются с использованием руководящих документов Федеральной
службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации.

4.8. Размещение информационных систем персональных данных, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.9. При обработке персональных данных в информационной системе персональных данных должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачи их лицам, не имеющим права доступа к такой информации;

б) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль уровня защищенности персональных данных.

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

а) мероприятия, изложенные в п. 1.6. настоящего Положения;

б) классификацию информационных систем персональных данных.

При этом, для каждой информационной системы персональных данных проводится:

разработка плана графика работ по обеспечению безопасности персональных данных (при разработке – до ввода в эксплуатацию);

определение угроз безопасности персональных данных при их обработке, определение перечня актуальных угроз, формирование на их основе модели угроз;

формирование организационно-технических требований к подсистеме защиты персональных данных на основе перечня актуальных угроз и установленного класса информационной системы персональных данных. Разработка на основе сформированных организационно-технических требований к подсистеме защиты персональных данных и установленного класса информационной системы персональных данных мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных;

проверка возможности использования средств защиты информации в информационной системе персональных данных, в т.ч. наличие действующего сертификата соответствия, специального защитного знака, назначения средства защиты информации, указанному в паспорте и сертификате;

установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.

в) обучение работников учреждения, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними.

г) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

д) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые привели к нарушению конфиденциальности персональных данных, снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению последствий подобных нарушений.

е) оценка соответствия информационных систем персональных данных учреждения требованиям безопасности персональных данных.

4.12. При обнаружении нарушений порядка обработки персональных данных, порядка работы технических средств обработки персональных данных ответственное должностное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы и докладывает о нарушениях непосредственному начальнику. После выявления причин нарушений и их устранения, предоставление персональных данных возобновляется.

4.13. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров, определенных Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации в пределах их компетенции.

4.14. Порядок эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются с учетом нормативных правовых документов Федеральной службы безопасности Российской Федерации.

4.15 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, которая создается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн и утверждается руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

4.16 Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

4.17 Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору и/или по персональному паролю.

4.18 Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

4.19 При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

4.20 Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;
- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

4.21 Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;
- вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких

магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

4.22 Лица, ответственные за защиту персональных данных в медицинской информационной системе персональных данных «ВебМИС» государственного бюджетного учреждения Ростовской области «Стоматологическая поликлиника № 1» в г. Ростове-на-Дону:

Ответственный за обработку ПДн - штатный сотрудник определяющий уровень доступа и ответственность лиц, участвующих в обработке ПДн. Назначается приказом по учреждению.

Ответственный за обеспечение безопасности персональных данных – штатный сотрудник, отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн. Назначается приказом по учреждению.

Администратор информационной безопасности – штатный сотрудник, ответственный за защиту медицинской информационной системы персональных данных «ВебМИС» государственного бюджетного учреждения Ростовской области «Стоматологическая поликлиника № 1» в г. Ростове-на-Дону от несанкционированного доступа (НСД) к информации. Назначается приказом по учреждению.

5. Обеспечение безопасности персональных данных, обрабатываемых без использования средств автоматизации

5.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, а также документируемые в результате автоматизированной обработки персональные данные, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители, документы), в специальных разделах или на полях форм (бланков).

5.2. При фиксации персональных данных 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, а также документируемых в результате автоматизированной обработки персональных данных, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) 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, а также документируемых в результате автоматизированной обработки персональных данных, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных

данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, а также документируемых в результате автоматизированной обработки персональных данных – при необходимости получения письменного согласия на обработку персональных данных (в случае, если такое согласие не давалось ранее);

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится учреждения или его подразделения, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена приказом руководителя учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится учреждение или его подразделение, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится учреждением или его подразделение.

5.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть

приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных 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;

б) 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.

5.6. 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).

5.7. Правила, предусмотренные пунктами 5.5 и 5.6 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации, а также документируемых в результате автоматизированной обработки персональных данных, 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.

5.9. Обработка персональных данных, осуществляемая без использования средств автоматизации, а также документируемых в результате автоматизированной обработки персональных данных, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей).

5.10. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.11. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации, а также документируемых в результате автоматизированной обработки персональных данных, включают в себя:

а) мероприятия, изложенные в п. 1.6. настоящего Положения;

б) при хранении документов, содержащих персональные данные, должны соблюдаться условия, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним, а именно, такие документы должны храниться в опечатываемых сейфах, а при их отсутствии – в запирающихся на ключ индивидуальных шкафах;

в) должна быть исключена возможность случайного или преднамеренного несанкционированного просмотра документов, содержащих персональные данные;

г) на документах (в необходимых случаях и на их проектах), содержащих персональные данные, может проставляться пометка "Для служебного пользования", поскольку персональные данные являются сведениями, конфиденциального характера.