«Утверждаю»
Директор ООО «Дент-имплант»
_____ Ко Бон Хак
«_13_»__ноября_____2012г.

Положение о порядке обработки и защиты персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение о порядке обработки персональных данных пациентов (далее - Положение) стоматологического центра «Дент-имплант» разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федеральным законом от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

1.2. Цель разработки Положения - определение порядка получения, обработки, хранения, передачи и любого другого использования персональных данных пациентов стоматологического центра «Дент-имплант», обеспечение защиты прав и свобод пациентов стоматологического центра при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным пациентов стоматологического центра, за невыполнение норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента введения его в действие приказом директора и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом директора.

1.4 Все работники стоматологического центра должны быть ознакомлены с настоящим Положением под роспись (Приложение 1).

1.5 При достижении целей обработки, информация, содержащая сведения ограниченного доступа (персональные данные) попадает под действие Архивного законодательства и иных федеральных законов РФ.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В настоящем Положении в соответствии со статьей 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» используются следующие основные понятия:

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

-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;

- 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;

- 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;
2.2 В состав персональных данных пациентов стоматологического центра входят документы, содержащие информацию о паспортных данных, образовании, семейном положении, месте жительства, контактных номерах телефона, состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью, реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), номера удостоверений, подтверждающих право на льготу при постановке зубных протезов (удостоверения пенсионера, ветерана труда, реабилитированного, труженика тыла).
2.3.1. Информация, представляемая пациентом при оформлении на прием к врачу в стоматологическом центре, должна иметь документальную форму. При оформлении первичной документации (медицинская карта стоматологического больного (форма №043/у), лицо, обратившееся за медицинской помощью, предъявляет медицинскому регистратору, менеджеру:
- паспорт или иной документ, удостоверяющий личность;
- ИНН;
- страховое свидетельство государственного пенсионного страхования (СНИЛС);
- медицинский страховой полис ОМС (ДМС);
- флюорография органов грудной клетки. В отдельных случаях, с учетом специфики работы, федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации и постановлениями Правительства Хабаровского края может предусматриваться необходимость предъявления при оформлении пациента на прием дополнительных документов (в том числе документы, подтверждающие льготу: пенсионное удостоверение, удостоверение ветерана труда, реабилитированного и т.п.).
2.3.2. При оформлении пациента на прием к стоматологу работником регистратуры стоматологического центра заполняется унифицированная форма №043/у «Медицинская карта стоматологического больного», в которой отражаются следующие анкетные и биографические данные пациента:
- общие сведения (Ф.И.О. пациента, дата рождения (возраст), пол (м, ж), сведения о месте жительства, контактных телефонах, место работы, профессия, перенесенные и сопутствующие заболевания);
- сведения о социальных гарантиях (пенсионер и т.п.)
В дальнейшем в медицинскую карту вносятся:
- диагноз;
- жалобы;
- развитие настоящего заболевания;
- данные объективного исследования, внешний осмотр;
- данные рентгеновских лабораторных исследований;
- план обследования;
- план лечения;
- консультация;

- запись о проделанной работе, с указанием даты и подписи врача.
2.3.3. В регистратуре стоматологического центра создаются и хранятся следующие группы документов, содержащие данные о пациентах в единичном или сводном виде:
2.3.3.1. Документы, содержащие персональные данные пациентов (медицинская карта стоматологического больного).
2.3.3.2. Хранение групп документов осуществляется:
- картотека (медицинские карты) – в шкафу регистратуры;
3. СБОР, ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ
3.1 Порядок получения персональных данных.
3.1.1. Все персональные данные пациента следует получать у него самого. 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.
3.1.2. Стоматологический центр не имеет права получать и обрабатывать персональные данные пациента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.
3.1.3. Стоматологический центр вправе обрабатывать персональные данные пациентов только с их письменного согласия. Бланк письменного согласия пациента на обработку своих персональных данных представлен в Приложении 2 к настоящему Положению. Бланк письменного согласия несовершеннолетнего пациента на обработку его персональных данных представлен в Приложении 3 к настоящему Положению.
3.2. Обработка персональных данных пациентов, содержащихся в информационной системе персональных данных, считается автоматизированной, так как производится с помощью средств вычислительной техники.
3.3. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия пациентам в получении медицинской помощи, контроля количества и качества выполняемой работы и обеспечения безопасности при получении медицинской помощи.
3.4. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться федеральными законами и локальными актами ООО «Дент-имплант».
3.5. При принятии решений, затрагивающих интересы пациента, стоматологический центр не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
3.6. Персональные данные пациентов при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).
3.7. При фиксации персональных данных пациентов на материальных носителях не допускается фиксация на одном материальном носителе персональных данных пациентов, цель обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных пациентов, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
3.8. При несовместимости целей обработки персональных данных пациентов, 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:
- при необходимости использования или распространения определенных персональных данных пациентов 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 пациента.
- 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.
3.9. Уничтожение или обезличивание части персональных данных пациентов, 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).
3.10. Правила, предусмотренные пунктами 3.8. и 3.9 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными пациентов.
3.11. Уточнение персональных данных 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 пациента.
3.12. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных пациентов можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных пациентов, либо имеющих к ним доступ. утвержден приказом директора на основании утвержденного штатного расписания.
3.13. Необходимо обеспечивать раздельное хранение персональных данных пациентов, обработка которых осуществляется в различных целях.
3.14. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных пациентов и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.
3.15. Защита персональных данных пациента от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральными законами.
3.16. Во всех случаях отказ пациента от своих прав на сохранение и защиту тайны недействителен.
3.17. Лицам, имеющим право и/или обязанность осуществлять обработку персональных данных в информационных системах персональных данных стоматологического центра (далее – ИСПДн), администратор ИСПДн предоставляет уникальный логин и пароль для доступа к соответствующей ИСПДн. Доступ предоставляется в объеме, соответствующем должностным инструкциям работников.
Информация может вноситься как в автоматическом режиме – при уточнении, извлечении, использовании и передаче на машиночитаемом носителе информации, так и в ручном режиме – при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую обработку.
4. ПЕРЕДАЧА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.
4.1. При передаче персональных данных пациента оператор должен соблюдать следующие требования:
4.1.1. Не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья пациента, а также в случаях, установленных федеральным законом.
4.1.2. Не сообщать персональные данные пациента в коммерческих целях без его письменного согласия. Обработка персональных данных пациентов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.
4.1.3. Предупредить лиц, получивших 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, получившие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных пациентов в пределах стоматологического центра в соответствии с настоящим Положением:
4.1.4.1. Регистратор, менеджер стоматологического центра персональные данные пациентов передают лично лечащему врачу, администратору ИСПДн, директору стоматологического центра.
4.1.4.2. Регистратор, менеджер стоматологического центра персональные данные пациентов могут передавать лечащему врачу, администратору ИСПДн, директору стоматологического центра через информационную систему путем занесения персональных данных в компьютерную программу, доступ к которой имеется только у лиц, допущенных к работе с информацией, содержащей персональные данные пациентов.
4.1.4.3. Разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции. 4.1.5. Передача персональных данных за пределы стоматологического центра осуществляется во исполнение обязательств по работе в системе ОМС (ДМС) с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа.
4.2. Хранение персональных данных пациентов.
4.2.1. Персональные данные пациентов на бумажных носителях обрабатываются и хранятся в регистратуре, комнате медицинского персонала.
4.2.2. Персональные данные пациентов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
4.3. При получении персональных данных не от пациента (за исключением случаев, если персональные данные были предоставлены стоматологическому центру на основании федерального закона или если персональные данные являются общедоступными) стоматологический центр до начала обработки таких персональных данных обязан 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 настоящим Федеральным законом права субъекта персональных данных.
4.4. Хранение персональных данных осуществляется в порядке, исключающем бесконтрольный доступ к ним, их утрату или неправомерное использование. Документы, содержащие персональные данные, должны храниться в надежно запираемых хранилищах; также допускается их хранение в не запираемых шкафах (ящиках), при условии, что бесконтрольный доступ посторонних лиц в помещения исключен.
Помещения, в которых ведется обработка персональных данных, должны обеспечивать их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц. В течение рабочего дня ключи от шкафов (ящиков, хранилищ), в которых содержатся персональные данные (носители персональных данных), а также помещений, где находятся средства вычислительной техники, предназначенные для обработки и хранения персональных данных, находятся на хранении у ответственных работников. По окончании рабочего времени такие помещения должны быть закрыты на ключ, бесконтрольный доступ в них должен быть исключен (например, путем опечатывания, использования системы видеонаблюдения, систем контроля доступа и т.д.).
Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.
Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.
Срок хранения персональных данных, внесенных в ИСПДн, должен соответствовать сроку хранения бумажных носителей персональных данных.

5. СРОКИ И ПОРЯДОК ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Срок обработки персональных субъектов персональных данных осуществляется в течение всего периода лечения, (срока трудового договора).
5.2. Хранение документов, содержащих персональные данные осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов.
5.3. Персональные данные хранятся в структурных подразделениях, к функциональным обязанностям которых относится обработка соответствующих персональных данных.
5.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях, в специальных разделах или на полях форм (бланков).
5.5. Должно обеспечиваться раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами.
5.6. Контроль за хранением и использованием материальных носителей, содержащих персональные данные, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляет руководитель стоматологического центра.

6. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

6.1. Лицами, ответственными за обработку документов в стоматологическом центре, осуществляется систематический контроль за выделением документов на бумажных носителях, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.
6.2. Вопрос об уничтожении документов, содержащих персональные данные, по истечении срока их хранения, рассматривается на заседании экспертной комиссии. Состав экспертной комиссии утверждается приказом директора.
6.3. На основе представленного лицом, ответственным за обработку документов, в экспертную комиссию стоматологического центра акта о выделении документов к уничтожению выносится решение о его согласовании (несогласовании).
6.4. По итогам заседания экспертной комиссии составляется протокол и делаются соответствующие записи в акте о выделении к уничтожению документов, затем акт представляется на утверждение директору.
6.5. Контроль за процедурой уничтожения документов осуществляется директором. Сведения об уничтожении вносятся в акт о выделении к уничтожению документов.
6.6. Уничтожение персональных данных на электронных носителях производится под контролем лица, ответственного за обработку персональных данных, путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

7. РАССМОТРЕНИЕ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

7.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
7.1.1. подтверждение факта обработки персональных данных;
7.1.2. правовые основания и цели обработки персональных данных;
7.1.3. применяемые способы обработки персональных данных;
7.1.4. сведения о наименовании и месте нахождения Института;
7.1.5. сведения о лицах (за исключением гражданских служащих), которые имеют доступ к персональным

данным или которым могут быть раскрыты персональные данные на основании договора с стоматологическим центром;
7.1.6. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации в области персональных данных;
7.1.7. сроки обработки персональных данных, в том числе сроки их хранения в стоматологическом центре;
7.1.8. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
7.1.9. информацию об осуществленной или предполагаемой трансграничной передаче данных;
7.1.10. наименование организации или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению стоматологического центра, если обработка поручена или будет поручена такой организации или лицу;
7.1.11. иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
7.2. Субъект персональных данных в соответствии с частью 1 статьи 14 Федерального закона "О персональных данных" вправе обращаться в Институт с требованием об уточнении его персональных данных, о блокировании или уничтожении персональных данных 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.
7.3. Сведения, касающиеся обработки персональных данных, предоставляются в доступной форме. В таких сведениях не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
7.4. Сведения, касающиеся обработки персональных данных, предоставляются по письменному запросу субъекта персональных данных или его представителя на имя директора. Запрос должен содержать:
7.4.1. номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
7.4.2. сведения, подтверждающие участие субъекта персональных данных в правоотношениях с ООО «Дент-имплант» (договор и т.п.), либо сведения, иным образом подтверждающие факт обработки персональных данных в ООО «Дент-имплант», подпись заинтересованного субъекта персональных данных или его представителя.
К запросу, направленному представителем субъекта персональных данных, должен прилагаться документ (надлежащим образом заверенная копия), подтверждающий его полномочия.
Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
7.5. В случае, если сведения, касающиеся обработки персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в целях получения указанных сведений 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 законодательством Российской Федерации в области персональных данных, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
Субъект персональных данных вправе, обратиться повторно в стоматологический центр или направить повторный запрос в целях получения сведений, касающихся обработки персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения указанного срока 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 должен содержать обоснование направления повторного запроса.

Субъекту персональных данных может быть отказано в выполнении повторного запроса, не соответствующего установленным требованиям. Такой отказ должен быть мотивированным.
Право субъекта персональных данных на доступ к его персональным данным ограничено в соответствии с пунктами 3 и 4 части 8 статьи 14 Федерального закона "О персональных данных", если обработка его персональных данных в стоматологическом центре ООО «Дент-имплант» осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.
7.6. В случае отказа в предоставлении информации дается мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона "О персональных данных" или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения заинтересованного субъекта персональных данных или его представителя либо с даты получения запроса.

8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ ПАЦИЕНТА.
8.1. Право доступа к персональным данным пациента имеют лица, указанные в утвержденном приказом директора на основании утвержденного штатного расписания.
8.2. Пациент стоматологического центра имеет право:
8.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные.
8.2.2. Требовать от лечебного учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для стоматологического центра персональных данных.
8.2.3. Получать от стоматологического центра
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.
8.2.4. Требовать извещения от стоматологического центра всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
8.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия стоматологического центра при обработке, защите его персональных данных.
8.3. Копировать и делать выписки персональных данных пациента разрешается исключительно в служебных целях с письменного разрешения директора стоматологического центра.
8.4. Передача информации третьей стороне возможна только при письменном согласии пациента.
8.5. Органы прокуратуры в связи с осуществлением ими прокурорского надзора вправе получать доступ к персональным данным, а также к сведениям, составляющим врачебную тайну, без согласия пациента или его законного представителя.
9. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЗА ДОСТОВЕРНОСТЬ ВНОСИМЫХ В ИНФОРМАЦИОННУЮ СИСТЕМУ ПЕРСОНАЛЬНЫХ ДАННЫХ.
9.1 Сотрудники, допущенные к обработке персональных данных, обязаны:
- знать и выполнять требования настоящего Положения;
- осуществлять обработку персональных данных в целях, определенных законодательством Российской Федерации и организационно-распорядительными документами Учреждения (Филиала);
- знакомиться только с теми персональными данными, к которым им разрешен доступ;

-не разглашать известные им персональные данные, информировать своего непосредственного начальника о фактах нарушения порядка обработки персональных данных и о попытках несанкционированного доступа к ним;
- предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены
- выполнять требования по защите полученных персональных данных;
- соблюдать правила пользования документами, содержащими персональные данные, порядок их обработки и защиты;
- предоставлять письменные объяснения о допущенных нарушениях установленного порядка обработки персональных данных, а также о фактах их разглашения или утраты;
- нести ответственность за достоверность внесенных персональных данных в информационную систему, либо на материальные носители.
9.2 Форма уведомления об особенностях обработки персональных данных (Приложение 6).

10. ОТВЕТСТВЕННОСТЬ ПАЦИЕНТОВ ЗА ДОСТОВЕРНОСТЬ ПРЕДСТАВЛЯЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ:
10.1. В целях обеспечения достоверности персональных данных субъекты персональных данных - пациенты обязаны:
10.1.1. При первичном обращении в стоматологический центр предоставлять сотрудникам центра достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.
10.1.2. В случае изменения персональных данных пациента: фамилия, имя, отчество, адрес места жительства, паспортные данные и др. сообщать об этом в стоматологический центр в течение 5 рабочих дней с даты их изменений.

11. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:
11.1. Сотрудники стоматологического центра, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациентов, несут дисциплинарную ответственность, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами и другими нормативными правовыми актами Российской Федерации.
11.2. Директор стоматологического центра несет административную ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных пациента, согласно Кодексу об административных правонарушениях Российской Федерации, а также возмещают пациенту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные пациента.
11.3. Сотрудники стоматологического центра несут персональную ответственность за сохранность носителей и обеспечение конфиденциальности персональных данных, ставших им известными в ходе исполнения служебных обязанностей, в том числе после окончания работы в стоматологическом центре.
11.4. За неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными или порядка обеспечения безопасности персональных данных к нему могут быть применены дисциплинарные взыскания, предусмотренные Трудовым кодексом Российской Федерации (ст. 192, ст.81), а именно: замечание, выговор, увольнение с работы.
11.5. Утрата документов, содержащих персональные данные, либо незаконное использование, получение и разглашение таких сведений влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

12. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: Обеспечение безопасности персональных данных, обрабатываемых в стоматологическом центре, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по их защите:

- определение актуальных угроз безопасности персональных данных, в том числе при их обработке в ИСПДн;
- применение организационных и технических мер по обеспечению безопасности персональных данных, в том числе при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает необходимый уровень защищенности персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности информации;
- учет машинных носителей персональных данных;
- обеспечение функционирования средств обработки персональных данных, а также средств защиты информации в соответствии с эксплуатационной и технической документацией;
- установление правил доступа к персональным данным, в том числе обрабатываемым в ИСПДн, а также обеспечение регистрации и учета действий, совершаемых с персональными данными;
- обнаружение и регистрация фактов несанкционированного доступа к персональным данным, несанкционированной повторной и дополнительной записи информации после ее извлечения из ИСПДн;
- восстановление персональных данных, модифицированных или удаленных (уничтоженных) вследствие несанкционированного доступа к ним
- контроль, за принимаемыми мерами по обеспечению безопасности персональных данных и защищенностью ИСПДн.

Актуальные угрозы безопасности персональных данных определяются в соответствии с моделью угроз и нарушителя безопасности персональных данных при их обработке в стоматологическом центре (далее – модель угроз и нарушителя). Типовая модель угроз и нарушителя утверждается приказом директора.

Защита персональных данных обеспечивается путем применения комплекса организационных и технических мер по обеспечению безопасности персональных данных. Типовые Меры по обеспечению защищенности персональных данных, обрабатываемых в стоматологическом центре, утверждаются приказом директора.

Лица, ответственные за организацию обработки персональных данных, должны осуществлять контроль за соблюдением правил обработки персональных данных, в том числе в ИСПДн. Администратор ИСПДн должен:
- соблюдать требования по обеспечению информационной безопасности при работе с ИСПДн;
- немедленно оповещать ответственного, за обеспечение информационной безопасности при обнаружении фактов несанкционированных действий с персональными данными;
- производить восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированных действий с ними.

Ответственный, за обеспечение информационной безопасности должен:
- осуществлять контроль доступа к персональным данным, обрабатываемым в ИСПДн;
- согласовывать заявки на доступ к функциям ИСПДн;
- осуществлять периодический контроль правильности назначения полномочий доступа к ИСПДн администраторами ИСПДн;
- осуществлять проверку учета действий по доступу к ресурсам ИСПДн;
- своевременное обнаруживать факты несанкционированного доступа к персональным данным и немедленное доводить такую информацию до ответственного за организацию обработки персональных данных и руководства стоматологического центра;
- не допускать воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
-осуществлять контроль, за обеспечением уровня защищенности персональных данных;
- осуществлять контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- осуществлять учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- осуществлять учет носителей персональных данных;
-проводить разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, нарушения правил эксплуатации средств защиты

информации, нарушения правил разграничения доступа к персональным данным, нарушения правил работы с персональными данными, любых других нарушений, приводящих к снижению уровня защищенности персональных данных, принимать меры по предотвращению возможных последствий нарушений правил обработки персональных данных.

13. ТРЕБОВАНИЯ ПО УЧЁТУ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ:

На всех объектах информатизации стоматологического центра должен быть обеспечен учет машинных носителей информации, используемых для хранения и обработки персональных данных.

Обязательному учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- машинные носители информации, встроенные в средства вычислительной техники (накопители на жестких дисках);
- портативные вычислительные устройства со встроенными носителями информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства).

Учет машинных носителей включает присвоение им регистрационных номеров. Для идентификации машинных носителей информации могут использоваться серийные номера, присвоенные производителями, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера. Регистрационный номер наносится на несъемную часть корпуса носителя информации.

Учет всех типов машинных носителей информации или, при невозможности, целиком портативных вычислительных устройств, ведется в журнале учета машинных носителей информации и портативных вычислительных устройств (Приложение 5).

Учёт носителей информации, использующихся в ИСПДн, контроль правил хранения носителей информации и ведение журнала возлагается на ответственного за информационную безопасность.

При регистрации носителей информации (до первой записи на них персональных данных) должна указываться следующая информация:

- ограничительная пометка доступа («ПДн» или «ДСП»);
- ответственный за использование / владелец носителя информации;
- идентификатор носителя информации. Должен быть организован регулярный контроль наличия учтенных носителей информации.

14. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

Событие информационной безопасности – какое-либо событие, идентифицированное появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент информационной безопасности – одно событие или группа событий информационной безопасности, которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности персональных данных.

Процедура реагирования на инциденты информационной безопасности определяет действия работников стоматологического центра в случае возникновения нештатных ситуаций в процессе обработки персональных данных в ИСПДн. Эти действия обязательны для исполнения всеми должностными лицами в части выполнения вмененных им обязанностей.

15. ТРЕБОВАНИЯ И ПРАВИЛА РЕГИСТРАЦИИ И УЧЕТА ДЕЙСТВИЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ:

Целью регистрации событий безопасности является обнаружение несанкционированных действий, связанных с обработкой персональных данных. Мониторинг систем следует проводить с целью проверки эффективности применяемых мер и средств контроля и управления.

Перечень событий безопасности, подлежащих регистрации (при наличии технической возможности):

- вход (выход), а также попытки входа субъектов доступа в ИСПДн;
- попытки удаленного доступа в ИСПДн;
- запуск (остановка) ИСПДн;
- подключение машинных носителей информации к средствам обработки информации;
- вывод информации на носители информации (в т.ч. на печать);
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;
- заведение пользователя ИСПДн;
- блокирование пользователя ИСПДн;
- аннулирование (постоянное блокирование) пользователя ИСПДН;
- удаление пользователя ИСПДн;
- редактирование пользователя ИСПДн;
- изменение полномочий пользователя ИСПДн;
- ошибка ввода пароля пользователя ИСПДн;
- изменение пароля пользователя ИСПДн;
- сброс пароля пользователя ИСПДн;
- изменение прав доступа к защищаемым объектам ИСПДн;
- удаление (очистка) журнала безопасности ИСПДн;
- невозможность (ошибка) записи в журнал безопасности;
- использование привилегий (работа с использованием привилегированных учетных записей);
- нарушения (попытки) политик доступа;
- предупреждения или отказы ИСПДн и их компонентов;
- изменения (попытки) параметров настройки системы безопасности и мер и средств контроля и управления.

При необходимости указанный перечень может быть адаптирован для каждой ИСПДн в зависимости от имеющихся технических возможностей и исходя из возможных способов реализации угроз безопасности информации для соответствующей ИСПДн.

Перечень должен анализироваться не реже одного раза в год, при начале эксплуатации новых ИСПДн, а также при существенных изменениях в модели угроз и (или) нарушителя безопасности информации.

В общем случае записи журналов безопасности должны храниться не менее 3 месяцев, причем в оперативном доступе (онлайн) – не менее 2 недель. Для различных событий ИСПДн сроки хранения соответствующих записей могут отличаться.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить следующие возможности по идентификации:

- даты и времени события безопасности;
- типа и описания события безопасности;
- субъекта доступа (пользователь и (или) процесс), связанного с данным событием безопасности;
- объекта доступа (защищаемый ресурс, внешнее устройство и т.д.);
- способа, средства доступа, используемых технологий доступа;
- результата события безопасности (успешно или неуспешно).

В ИСПДн сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);
- хранение информации о событиях.

16. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ:

Целью резервного копирования персональных данных является обеспечение возможности их восстановления в кратчайшие сроки в случае утраты (уничтожения).

Резервное копирование осуществляется путем регулярного создания резервных и архивных копий обрабатываемой в ИСПДн информации.

Резервное копирование данных, обрабатываемых в ИСПДн, осуществляется уполномоченным сотрудником, в должностные обязанности которого входят функции по обеспечению работоспособности данной ИСПДн или функции по резервному копированию информации.

Для создания резервных копий могут использоваться сервер резервного копирования, компактные (сменные) носители информации (CD/DVD-диски, внешние жесткие диски и т.п.), иные внешние носители информации, зарегистрированные установленным порядком.

Резервному копированию и хранению подлежат персональные данные, обрабатываемые в ИСПДн, а также иная информация, определяемая как критичная для обеспечения бесперебойной работы ИСПДн.

Резервное копирование производится в соответствии с регламентом резервного копирования, в котором определяются, в том числе, периодичность и виды проводимого резервного копирования, время запуска процедуры.

Выбор способа резервирования информации определяется в зависимости от следующих факторов:

- частоты обновления данных, подлежащих резервному копированию;
- заданной «давности» информации, восстанавливаемой с резервной копии в любой момент времени;
- возможности восстановления данных не с резервной копии, а по входной информации или дистрибутивам;
- максимального интервала недоступности данных.

Например, резервное копирование может осуществляться не реже одного раза в неделю. Сеансы резервного копирования настраиваются на внерабочее время с учетом возможности ИСПДн поддерживать работу с копируемыми данными, а также длительности выполнения процедуры резервного копирования. Полная резервная копия, являющаяся основным источником восстановления персональных данных, производится на внешнее хранилище информации, по возможности, отдаленное от ресурсов, на которых хранятся и обрабатываются резервируемые персональные данные.

Полная резервная копия содержит:

- информацию, необходимую для восстановления работоспособности ИСПДн;
- информацию, содержащуюся в ИСПДн;
- рабочие копии установочных компонентов (дистрибутивов) программного обеспечения рабочих станций;
- файлы конфигурации ИСПДн;
- прочую необходимую информацию.

Также должны быть определены правила хранения резервных копий, процедуры восстановление данных.

Восстановление информации из резервных копий может осуществляться в случаях:

- потери данных;
- необходимости исправления ошибочных операций с данными;
- тестового восстановления.