Утверждено
приказом главного врача
ГАУЗ «Детская клиническая
стоматологическая поликлиника №2»
№_____ от _____

ПОРЯДОК
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ ГАУЗ «ДЕТСКАЯ КЛИНИЧЕСКАЯ СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА №2»

1 Общая часть

1.1 Настоящий Порядок определяет порядок создания, обработки и защиты персональных данных пациентов ГАУЗ «Детская клиническая стоматологическая поликлиника №2» (далее - Учреждение-оператор).

1.2 Основанием для разработки данного локального нормативного акта являются:

- Конституция РФ от 12 декабря 1993 г. (ст. 2, 17-24, 41);
- часть 1 и 2, часть 4 Гражданского кодекса РФ;
- Указ Президента РФ от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Закон РФ от 28 июня 1991 г. № 1499-1 «О медицинском страховании граждан в Российской Федерации»;
- Федеральный закон от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 03 ноября 2006 г. № 174-ФЗ «Об автономных учреждениях»;
- Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах

персональных данных»;

1.3 Настоящий Порядок разработан в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в информационных системах персональных данных (далее по тексту «ИСПДн»).

1.4 Целью настоящего Порядка является формирование общих правил для обеспечения защиты Учреждением персональных данных (далее по тексту «ПДн») от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее по тексту «УБПДн»).

1.5 Порядок является обязательным для исполнения всеми работниками учреждения, имеющими доступ персональным данным.

2 Понятия и состав персональных данных.

Для целей настоящего Порядка применяются следующие термины и определения:

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.

Пациенты (субъекты персональных данных) - физические лица, обратившиеся к Учреждению-оператору с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Учреждением-оператором по вопросам получения медицинских услуг.

Врачебная тайна - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

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

Документы, содержащие персональные данные пациента - документы, необходимые для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений.

Обработка персональных данных пациента - 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 пациента.

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.

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

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.

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

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

Конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

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

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

Персональные данные пациента – это любая информация о пациенте и членах его семьи, полученная при обращении за медицинской помощью, обследовании и лечении (фамилия, имя, отчество, год, месяц, рождения, дата и место рождения, адрес регистрации и место проживания, пол, место работы, данные документов, удостоверяющие личность, ИНН, СНИЛС, данные полиса ОМС и ДМС, данные о состоянии здоровья, составляющие врачебную тайну, другая информация.

Информация ограниченного доступа -информация, доступ к которой ограничен федеральными законами.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Безопасность персональных данных - состояние защищённости ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке ИСПДн.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое прибывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Неавтоматизированная обработка персональных данных- обработка ПДн субъекта без использования средств вычислительной техники.

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

Клини́ческое иссле́дование — научное исследование с участием людей, которое проводится с целью оценки эффективности и безопасности нового лекарственного препарата или расширения показаний к применению уже известного лекарственного препарата.

3 Документы, содержащие персональные данные пациентов:

- медицинская карта стоматологического больного.
-талон амбулаторного пациента.
-лист учета на платные услуги.
-договор на оказание платных услуг, акты выполненных работ.
-листок нетрудоспособности.
-медицинские справки по запросам, предусмотренным законодательством.
-другие документы, учитывающие специфику работы медицинского учреждения.

4 Цель обработки персональных данных:

4.1 Оказание производственной деятельности учреждения (оказание

стоматологических услуг)
4.2 медицинский и статистический учет.
4.3 ведение кадровой работы и бухгалтерского учета.

5 Порядок получения, обработки и хранения, использования и передачи персональных данных пациентов, (в том числе и при проведении клинических исследований лекарственных препаратов).

5.1 Порядок получения, обработки персональных данных пациентов.

5.1.1.Все персональные данные предоставляются пациентом, или законным представителем пациента, для обработки добровольно. Если ПДн субъекта возможно получить только у третьей стороны, за исключением случаев, предусмотренных законодательством РФ, субъект должен быть уведомлен об этом заранее в письменном виде по почте работником, ответственным за организацию обработки и обеспечения безопасности ПДн, или другим сотрудником учреждения по его поручению. Работник учреждения, принимающий ПД-н субъекта, должен сообщить субъекту ПДн следующую информацию:
-Наименование, либо фамилия, имя отчество и адрес Учреждения или его представителя;
-Цель обработки ПДн и её правовое основание;
-Предполагаемые пользователи ПДн;
-Установленные действующим законодательством РФ права субъекта ПДн;
Работники Учреждения не имеют права получать и обрабатывать ПДн субъектов, не соответствующие целям их обработки.
5.1.2. Работники ГАУЗ «Детская клиническая стоматологическая поликлиника №2» имеют право запрашивать персональные данные пациента только в объеме, соответствующим перечню в «Уведомлении об обработке персональных данных», которое было предоставлено в Управление Роскомсвязьнадзора по Волгоградской области.
5.1.3. Обработка персональных данных пациентов ведется работниками на рабочих местах, выделенных для исполнения должностных обязанностей.
5.1.4. Копировать и предоставлять посторонним лицам полученные справочные и другие документы, содержащие персональные данные, запрещается.
5.1.5.Лица, получающие персональные данные пациентов для работы, соблюдать режим конфиденциальности. Данное требование не распространяется на обмен персональными данными субъектов персональных данных в порядке, установленном ФЗ.
5.1.6. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.
5.1.7. Передавать персональные данные представителям субъектов персональных данных в порядке установленном существующим

законодательством, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.
5.1.8. в соответствии с законодательством РФ в целях обеспечения прав и свобод человека и гражданина Учреждение и него представители при обработке ПДн субъекта должны соблюдать следующие общие требования:
-обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов РФ.
- при определении объема и содержания, обрабатываемых ПДн Учреждение должно руководствоваться действующим законодательством РФ н локальными нормативными актами Учреждения;
- при принятии решении, затрагивающих интересы субъекта , Учреждение не имеет права основываться на ПДн субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.
- защита ПДн субъекта от неправомерного их использования или утраты обеспечивается Учреждением в порядке, установленном действующим законодательством РФ.
-работники Учреждения должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки ПДп, а также об их правах и обязанностях в этой области.
-доступ Работников Учреждения к персональным данным субъектов ПДн в ИСПДн регламентируется только па основании локальных нормативных актах Учреждения с указанием перечня допущенных лиц, прав, доступа, необходимых для выполнения служебных обязанностей,
- обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой, категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц осуществляющих обработку ПДп либо имеющих к ним доступ;
- уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДп с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).
- уточнение ПДн 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 полого материального носителя с уточненными персональными данными;
- при хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДп и исключающие несанкционированный доступ к ним.
5.1.9. При передаче ПДн субъекта Работниками должны соблюдаться следующие требования:

- не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом;
- осуществлять передачу ПДн субъектов в пределах Учреждения в соответствии с нормативными документами внутреннего документооборота Учреждения.

5.1.10. Допускается передача ПДн субъектов сторонним организациям, если данная передача обусловлена Федеральным законом, либо соответствующим соглашением, и не нарушает прав субъекта ПДн.

5.2. Порядок хранения и использования персональных данных пациентов.

5.2.1. Персональные данные пациентов хранятся на бумажных постелях в специально предназначенных для этого запирающихся на ключ помещениях и доступны для определенного круга работников, с разграничением доступа к ним. В здании поликлиники установлена охранная и пожарная сигнализация, в нерабочее время в учреждение осуществляют охранные мероприятия работники охраны.

5.2.2.Персональные данные пациентов в электронном виде хранятся и информационной системе поликлиники. Технические средства, предназначенные для обработки персональных данных в том числе программно-технические средства и средства защиты информации, Должны соответствовать требованиям законодательства РФ о техническом регулировании.

5.2.3. В процессе хранения персональных данных пациент, в том числе и при проведении клинических исследований лекарственных препаратов, должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним. в соответствии с законодательством РФ и настоящим Порядком;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

5.3.Перечень должностей, имеющих доступ к персональным данным пациентов

5.3.1 Доступ к персональным данным пациентов имеют:

врач - стоматолог детский
зубной техник
медицинская сестра
медицинская сестра (стерилизационной)
врач - ортодонт

инженер
медицинская сестра (хирургического кабинета)
заведующий ортодонтическим отделением - врач - ортодонт
медицинский регистратор
врач - методист
главный бухгалтер
заведующий лечебно-профилактическим отделением - врач - стоматолог детский
гигиенист стоматологический
заведующий лечебно-профилактическим отделением - врач - стоматолог детский
врач - невролог
старшая медицинская сестра
логопед
медицинская сестра - анестезист
оператор электронно - вычислительных машин
врач - стоматолог хирург
врач - педиатр
программист
заведующий лечебно-профилактическим отделением - врач - стоматолог детский
медицинский психолог
врач - стоматолог терапевт
бухгалтер (1 квалификационный уровень)
оператор электронно - вычислительных машин
гигиенист стоматологический
заместитель главного врача по медицинской части
оператор электронно - вычислительных машин
кассир
врач - стоматолог
старшая медицинская сестра
специалист по кадрам
медицинская сестра - анестезист
рентгенолаборант
медицинская сестра (стерилизационной)
врач - анастезиолог - реаниматолог
медицинский статистик
врач - стоматолог - ортопед
заместитель главного врача по клинико-экспертной работе
врач челюстно - лицевой хирург
врач - отоларинголог
заведующий лечебно-профилактическим отделением - врач - стоматолог детский
врач - анастезиолог - реаниматолог
главный врач

5.3.2.Ответственным за организацию хранения,осуществление хранения, заполнение и выдачу персональных данных пациента на бумажных носителях, хранящихся в регистратуре, и рентгенологическом кабинете является заместитель главного врача по медицинской части.

5.3.3.Ответственным заорганизацию хранения,осуществлениехранения, использование, заполнение персональных данных пациента, хранящихся в бухгалтерии и кассе является главный бухгалтер.

5.3.4. Ответственными за организацию хранения, осуществление храпения персональных данных пациентов па электронных носителях являются программист и инженер.
5.3.5. Ответственным за организацию и хранения, осуществление хранения использование, заполнение персональных данных пациента, хранящихся в лечебных отделениях являются заведующие отделениями.
5.3.6.Ответственным за организацию хранения, осуществление хранения, использование, заполнение персональных данных пациента, используемые для работы в зуботехнической лаборатории является старший зубной техник.
5.3.7.Работники, перечисленные в п. 5.3.1. настоящего Порядка, имеют право получать только те персональные данные пациентов, которые необходимы им для выполнения своих должностных обязанностей.
5.3.8. Работники, перечисленные в п. 5.3.1. настоящего Порядка, обязаны соблюдать режим конфиденциальности и сохранение служебной тайны за пределами медучреждения.

5.4. Передача персональных данных пациента. .

5.4.1. Использование персональных данных пациента в пределах поликлиники осуществляется исключительно лицами, имеющими доступ к персональным данным пациентов, согласно перечня должностей в п. 5.3.1. настоящего Порядка и в соответствии с их должностными обязанностями;

5.4.2. При передаче персональных данных пациентов за пределы медучреждения должны быть соблюдены требования, обеспечивающие безопасность передачи персональных данных пациентов;
5.4.3. Не сообщать персональные данные пациента третьей стороне без оформления добровольного согласия на обработку персональных данных пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациенту а также в случаях, установленных федеральными законами.
5.4.4.Не сообщал, персональные данные пациента в коммерческих целях без его письменного добровольного согласия.
5.4.5. Работники, получающие персональные данные пациента, обязаны соблюдать режим конфиденциальности. Данный Порядок не распространяется на обмен персональными данными пациента в порядке, установленном федеральными законами Трудовым кодексом и Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

6. Организационные мероприятии по защите персональных данных при их обработке и передаче в информационных системах персональных данных.

6.1. В общем случае организационные мероприятия по защите ПДн связаны с формированием системы документов по защите ПДн, их

разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований.

6.2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в ИСПДп, и обеспечить запрет передачи ПДн по открытым каналам связи без применения установленных мер по се защите, а также исключить возможность внесения в контролируемую зону устройств регистрации и накопления информации без соответствующего разрешения.

6.3.Система документов по защите информации

6.3.1.Система документов по защите информации включает действующее законодательство РФ и локальные нормативные акты Учреждения.

6.3.2. Состав внутренних документов, разрабатываемых па основании действующего законодательства РФ и локальных нормативных актов Учреждения определяется на этапе приведения процессов обработки ПДн в Обществе в соответствие требованиям законодательства. Состав документов определяется Учреждением при возможном привлечении организации-лицензиатов.

6.3.3. В подразделении, обслуживающем ИСПДн, рекомендуется иметь комплект эксплуатационном и технической документации на ИСПДн, в том числе на систему защиты ПДн.

6.3.4. Обязанность поддерживать комплект документов но защите ПДн в актуальном состоянии возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДи.

6.4.Организационные мероприятия по защите ПДи, обрабатываемых на

6.4.1. Организационные мероприятия по защите ПДи, обрабатываемых на АРМ, должны быть связаны с обеспечением:

-сохранности машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;

-ограничения физического доступа и контроль доступа к изменению конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др);

-исключения возможностей несанкционированного просмотра изображении с монитора АРМ (терминала) через дверные проемы, окна - в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;

- режима блокирования доступа к АРМ (терминалу) во время отсутствия Пользователя;

-режима блокирования доступа в помещение с установленным АРМ (терминалом) во внерабочее время и в рабочее время при отсутствии Пользователя.

6.4.2.Организационные мероприятия по защите ПДн в локальных вычислительных сетях (далее по тексту «ЛВС») должны включать:

обеспечение режима запрета на вхождение в сеть под чужой учетной записью;

-обеспечение периодической смелы паролей Пользователями;

-обеспечение храпения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру подразделения (управления, отдела, группы и др.) и разрешения доступа к нему только Работников соответствующей структурной единицы;

-обеспечение файлового обмена информацией между Пользователями подразделений через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в ЛВС Пользователей;

-обеспечение создания для каждого пользователя локальной вычислительной сети личного сетевого каталога, предназначенного для хранения пользовательских данных, и предоставление ему всех прав (чтение, запись, создание, удаление, переименование) в отношении информации указанного каталога, за исключением права изменения привилегий доступа;

-обеспечение, контроля присвоения Пользователям учетных записей и их удаление или блокирование при увольнении Работника;

-обеспечение резервного копирования электронных информационных ресурсов;

-обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и АРМ.

6.5. Технические мероприятия по защите персональных данных.

6.5.1.Технические мероприятия по защите информации разрабатываются по результатам обследования объекта информатизации) предназначенного для обработки ПДн, и оценки возможностей реализации замысла защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения. Соответствующие требования излагаются в техническом задании на проектирование системы защиты.

6.5.2. Требуется осуществлять следующие технические мероприятия:

-применение сертифицированных программных и (или) аппаратных средств защиты информации от несанкционированного доступа, контроля целостности, регистрации н учета действии пользователей ИСПДн;

-применение сертифицированных средств криптографической защиты конфиденциальной информации при передаче но открытым каналам связи;

-предотвращение несанкционированной записи ПДн на съемные носители информации или вывода ПДн на печать;

-регулярный анализ защищенности системы защиты ПДн;
-защита ПДн при межсетевом взаимодействии;
-применение антивирусной защиты. Основными мерами, обеспечивающими безопасность хранения и использования персональных данных пациента, являются:

- реализация разрешительной системы допуска пользователей автоматизированных систем (АО) к персональным данным и связанным с их использованием документам;
- разграничение доступа пользователей АС к персональным данным, программным средствам их обработки;
- регистрация действии пользователей АС, контроль за доступом к персональным данным;
- учет и надежное храпение бумажных и машинных носителей персональных данных, исключающее их хищение, подмену или уничтожение;
- организация мер по резервному копированию персональных данных пациента для восстановления модифицированных или уничтоженных данных вследствие несанкционированного доступа к ним;
- размещение средств информатизации, используемых для обработки персональных данных, в запираемых помещениях, оснащенных охранной и пожарной сигнализациями;
-использование защитных мер для передачи персональных данных пациентов;
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр персональных данных посторонними лицами;
-предотвращение внедрения в АС компьютерных вирусов и программных закладок;
- ограничение доступа персонала учреждения и посторонних лиц в помещения, где хранятся носители персональных данных; организация физической защиты указанных помещений с помощью сил охраны и технических средств;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование

7.Обязанности Учреждении по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению блокированию и уничтожению персональных данных.

7.1. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя или уполномоченного органа но защите прав субъектов ПДн

должно быть осуществлено блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период внутренней проверки в учреждении.
7.2. В случае выявления неточных ПДн при обращении субъекта ПДп или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДп, должно быть осуществлено блокирование ПДп, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДп не нарушает права и законные интересы субъекта ПДн или третьих лиц.
7.3. В случае подтверждения факта неточности ПДп на основании сведении представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДп, или иных необходимых документов, должно быть проведено уточнение ПДн работником, ответственным за организацию обработки и обеспечение безопасности ПДн, либо обеспечено их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снято блокирование ПДн. Уточнение ПДп должно производиться на основании данных, полученных от субъекта ПДн.
7.4. В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДп лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДп, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Учреждение обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.
7.5. В случае достижения цели обработки ПДн Учреждение обязано прекратить обработку ПДп или обеспечить ее прекращение (если обработка ПДп осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДп осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДп, если иное не

предусмотрено договором, стороной которого, выгодоприобретателем или поручителем но которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн, либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.
7.6. В случае невозможности уничтожения ПДн в течение срока, указанного в п. 7.4 - 7.5, Учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен Федеральными законами.

8. Контроль состояния системы защиты персональных данных.

Общие вопросы контроля состояния защиты ПДн.
8.1.В рамках проверок состояния защиты ПДн рекомендуется осуществлять контроль: наличия в подразделениях нормативных документов по защите информации и доведения их до персонала с фиксацией факта ознакомления с документами; знания и выполнения работниками требовании локальных нормативных актов Учреждения по защите ПДн при их обработке в ИСПДн Учреждения; наличия и комплектности эксплуатационной и технической документации на систему защиты ПДн, а так же факта ознакомления работников Учреждения с инструкциями пользователей и администраторов средств защиты информации с соответствующей отметкой об ознакомлении в инструкциях; работоспособности системы защиты ПДп; задания требований небезопасности ПДн при разработке (модернизации) ИСПДн.
8.2. Контроль состояния защиты ПДн осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности ПДн. Работником (либо комиссией), назначаемым Учреждением.
8.3. Результаты проверок оформляются в виде отчетов о проведении проверки.

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

9.1.С каждым работником, использующим персональные данные пациента и сведения, составляющие служебную тайну, для выполнения своих должностных обязанностей, согласно перечня должностей и п.5.3.1 настоящего Порядка, заключается Договор о защите персональных данных пациентов и сохранении служебной тайны .
9.2.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, установленных действующим законодательством и настоящим Порядком, несут

дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.