УТВЕРЖДАЮ

Главный врач ГБУЗ «ОГПТД»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В.Логинов

«\_09\_\_» \_\_\_\_01\_\_\_\_\_\_\_ 2013г.

Положение

о защите персональных данных пациентов и работников ГБУЗ «ОГПТД».

1. Общие положения.

1.1. Настоящее Положение определяет порядок создания, обработки и защиты персональных данных пациентов и работников государственного бюджетного учреждения здравоохранения «Оренбургский городской противотуберкулезный диспансер» (далее по тексту – Учреждение).

1.2. Основанием для разработки настоящего положения:

- Конституция Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Гражданский кодекс Российской Федерации;

- федеральный закон от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

- федеральный закон от 8 января 1998 года № 3-ФЗ «О наркотических и психотропных веществах»;

- федеральный закон от 30 марта 1999 года № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»;

- федеральный закон от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- федеральный закон от 17 сентября 1998 года № 157-ФЗ «Об имуннопрофилактике инфекционных заболеваний»;

- постановление Правительства Российской Федерации от 21 марта 2012 года № 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 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных»;

- приказ ФСТЭК № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 3 февраля 2008 года «Об утверждении Порядка проведения классификации информационных систем персональных данных» (зарегистрировано в минюсте РФ от 3 апреля 2008 года № 11462);

- приказ ФСТЭК от 5 февраля 2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (зарегистрировано в Минюсте 19 февраля 2010 года № 16456);

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 14 февраля 2008 года);

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 года);

- Устав Учреждения;

- приказы главного врача в сфере защиты персональных данных.

1.3. Целью настоящего Положения является определение порядка обработки персональных данных пациентов Учреждения, а также лиц, работающих по трудовым и гражданско-правовым договорам (далее –работников) Учреждения, согласно Перечня персональных данных, утвержденного приказом главного врача; обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющим доступ к персональным данным пациентов и работников Учреждения, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.4. Персональные данные пациентов относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере служебной тайны.

2. Основные понятия, используемые в настоящем Положении.

Для целей настоящего Положения 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 с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Учреждением по вопросам получения медицинских услуг.

**Работники (субъекты персональных данных)** - физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением.

**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.

**Документы, содержащие персональные данные работника** - документы, которые работник предоставляет Учреждению (работодателю) в связи с трудовыми отношениями и касающиеся конкретного работника (субъекта персональных данных), а также другие документы, содержащие сведения, предназначенные для использования в служебных целях.

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

**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.

**Обработка персональных данных пациента или работника** - 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 или работника.

**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.

3. Общие принципы и условия обработки персональных данных пациентов и работников.

3.1. Обработка персональных данных пациентов и работников осуществляется на основе принципов:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

г) обработке подлежат только персональные данные, которые отвечают целях их обработки;

д) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждение должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом «О персональных данных», договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3.2. В целях обеспечения прав и свобод человека и гражданина, Учреждение и его представители при обработке персональных данных пациента или работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных пациента может осуществляться исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, оформления договорных отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну в соответствии с действующим законодательством.

3.2.3. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законодательства Российской Федерации в области персональных данных и иных нормативных правовых актов с учетом положений федерального закона «О персональных данных», оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, содействии работникам в трудоустройстве, обучении, повышении квалификации и продвижении по службе, обеспечении личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества работодателя;

3.2.3. Все персональные данные пациента следует получать у него самого или его уполномоченного представителя. Все персональные данные работника работодатель должен получать у него самого. Если персональные данные пациента или работника, возможно, получить только у третьей стороны, то пациент или работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

3.2.4. При определении объема и содержания, обрабатываемых персональных данных пациента или работника, Учреждение должно руководствоваться Конституцией РФ, Трудовым кодексом РФ, законодательством Российской Федерации в сфере охраны здоровья граждан и сфере защиты персональных данных и обработки информации, уставом Учреждения и иными федеральными законами и нормативными правовыми актами в области защиты персональных данных;

3.2.5. Учреждение не имеет права получать и обрабатывать персональные данные пациента или работника, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных федеральным законом «О персональных данных». В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

3.2.6. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении пациента и работника или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральным законом «О персональных данных»;

3.2.7. Решение, порождающее юридические последствия в отношении пациента или работника, или иным образом затрагивающее его права и законные интересы, может быть принято только на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме пациента и работника, или в случаях, предусмотренных действующим законодательством, устанавливающим также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных;

3.2.8. Учреждение обязано разъяснить пациенту и работнику порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражения против такого решения, а также разъяснить порядок защиты пациентом и работником своих прав и законных интересов.

3.2.9. Учреждение обязано рассмотреть возражение в течение тридцати дней со дня его получения и уведомить пациента и работника о результатах рассмотрения такого возражения.

3.2.10. Защита персональных данных пациентов и работников от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет своих средств в порядке, установленным федеральным законодательством и иными нормативными правовыми актами.

3.2.11. Работники или их представители должны быть ознакомлены под личную подпись с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3. Учреждение вправе поручить обработку персональных данных другому лицу с согласия пациента или работника, если иное не предусмотрено федеральным законом «О персональных данных», на основании заключенного с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные федеральным законом «О персональных данных». В поручении Учреждения должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 федерального закона «О персональных данных».

3.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, не обязано получать согласие пациента или работника на обработку его персональных данных.

3.5. В случае, если Учреждение поручает обработку персональных данных другому лицу, ответственность за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

4. Получение персональных данных пациента и работника.

4.1. Получение персональных данных преимущественно осуществляется путем представления их самим пациентов или работником, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством Российской Федерации.

4.2. В случаях, предусмотренных действующим законодательством Российской Федерации, обработка персональных данных осуществляется только с согласия пациента и работника в письменной форме. Равнозначным содержащему собственноручную подпись пациента и работника согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом «О персональных данных» электронной подписью. Согласие пациента и работника в письменной форме на обработку его персональных данных должно включать в себя, в частности:

а) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

б) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

в) наименование и адрес Учреждения, получающего согласие субъекта персональных данных;

г) цель обработки персональных данных;

д) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

е) наименование или фамилию, имя, отчества и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка будет поручена такому лицу;

ж) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;

з) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено действующим законодательством Российской Федерации;

и) подпись субъекта персональных данных.

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

В случае недееспособности пациента или недостижении пациентом возраста 15 лет согласие на обработку его персональных данных дает в письменной форме его законный представитель.

4.3. В случае необходимости проверки персональных данных пациента или работника, Учреждение заблаговременно должно сообщить об этом пациенты или работнику, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента или работника дать письменное согласие на их получение.

5.Хранение и использование персональных данных пациентов и работников.

5.1. Информация персонального характер пациента и работника хранится и обрабатывается с соблюдением требований действующего законодательства Российской Федерации о защите персональных данных.

5.2. Порядок хранения документов, содержащих персональные данные работников осуществляется в соответствии с:

- Правилами, устанавливающими порядок ведения и хранения трудовых книжек, а также порядок изготовления бланков трудовой книжки и обеспечения ими работодателей (утверждены Постановлением Правительства Российской Федерации от 16 апреля 2003 г. № 225 «О трудовых книжках);

- Унифицированными формами первичной учетной документации по учету труда и его оплаты (утверждены постановлением Госкомстата от 5 января 2004 г. № 1);

- федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

- Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения (утверждены Приказом Минкультуры России от 25 августа 2010 г. № 558).

5.3. Обработка персональных данных пациентов и работников Учреждения осуществляется смешанным путем:

а) неавтоматизированным способом обработки персональных данных;

б) автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

5.4. Персональные данные пациентов и работников хранятся на бумажных носителях и в электронном виде.

5.5. Хранение текущей документации и оконченной производством документации, содержащей персональные данные пациентов и работников Учреждения, осуществляется во внутренних подразделениях Учреждения, а также в помещениях Учреждения, предназначенных для хранения отработанной документации, в соответствии с приказом главного врача Учреждения.

Ответственные лица за хранение документов, содержащих персональные данные пациентов и работников, назначены приказом главного врача Учреждения.

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

Хранение документов, содержащих персональные данные пациентов и работников, осуществляется в течение установленных действующим законодательством Российской Федерации сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

5.7. Учреждение обеспечивает ограничение доступа к персональным данным пациентов и работников лицам, не уполномоченным действующим законодательством Российской Федерации либо Учреждением для получения соответствующих сведений.

5.8. Доступ к персональным данным пациентов и работников без специального разрешения имеют только должностные лица Учреждения, допущенные к работе с персональными данными пациентов и работников приказом главного врача Учреждения. Данным категориям работников в их должностные обязанности включается пункт об обязанности соблюдения требований по защите персональных данных.

6. Защита персональных данных пациентов и работников.

6.1. Учреждение при обработке персональных данных пациентов и работников обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2. Обеспечение безопасности персональных данных пациентов и работников достигается, в частности:

а) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

б) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

в) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

г) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

д) учетом машинных носителей персональных данных;

е) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

ж) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

и) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.3. Для обеспечения безопасности персональных данных пациентов и работников при неавтоматизированной обработке предпринимаются следующие меры:

6.3.1. Определяются места хранения персональных данных, которые оснащаются средствами защиты:

6.3.1.1. в кабинетах, где осуществляется хранение документов, содержащих персональные данные пациентов и работников, имеются сейфы, шкафы, стеллажи, тумбы;

6.3.1.2. дополнительно кабинеты, где осуществляется хранение документов, оборудованы замками и системами охранной и пожарной сигнализации;

6.3.1.3. Учреждение использует услуги вневедомственной охраны.

6.3.2. Все действия по неавтоматизированной обработке персональных данных пациентов и работников осуществляются только должностными лицами, согласно Списку должностей, утвержденного приказом главного врача Учреждения, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.3.3. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

6.3.3.1. при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) только копия;

6.3.3.2. 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

6.3.3.3. 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). Персональные данные пациентов и работников, содержащиеся на материальных носителях уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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.

6.3.4. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.4. Для обеспечения безопасности персональных данных пациента и работника при автоматизированной обработке предпринимаются следующие меры:

6.4.1. Все действия при автоматизированной обработке персональных данных пациентов и работников осуществляются только должностными лицами, согласно Списку должностей, утвержденного приказом главного врача Учреждения, и только в объеме, необходимым данным лицам для выполнения своей трудовой функции.

6.4.2. Персональные компьютеры, имеющие доступ к базам хранения персональных данных пациентов и работников, защищены паролями доступа. Пароли устанавливаются Администратором информационной безопасности и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов и работников на данном персональном компьютере.

6.4.3. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

6.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами главного врача Учреждения по архивному делу, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено действующим законодательством Российской Федерации.

7. Передача персональных данных пациентов и работников третьим лицам.

7.1. Передача персональных данных пациентов третьим лицам осуществляется Учреждением только с письменного согласия пациента, с подтверждающей визой главного врача, за исключением случаев, предусмотренных федеральных законом от 23 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». Лица, которым в установленном федеральным законом «О персональных данных» порядке переданы сведения, составляющие персональные данные пациента, несут дисциплинарную, административную или уголовную ответственность за разглашением в соответствии с действующим законодательством Российской Федерации.

7.2. Передача персональных данных пациента третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой главного врача Учреждения при соблюдении требований, предусмотренных пунктом 7.1 настоящего Положения.

7.3. При передаче персональных данных работника третьим лицам работодатель должен соблюдать следующие требования:

7.3.1. Не сообщать персональные данные работника третьему лицу без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях прямо предусмотренных действующим законодательством Российской Федерации.

7.3.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

7.3.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

7.3.4. Не запрашивать информацию о состоянии работника, за исключением тех сведений, которые относятся к возможности выполнения работником трудовой функции.

7.3.5. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и только в том объеме, который необходим для выполнения указанными представителями их функций.

7.4. Передача персональных данных работника третьим лицам осуществляется на основании письменного заявления (запроса) третьего лица с разрешающей визой главного врача Учреждения и только с согласия работника, в отношении которого поступил запрос, за исключением случаев, предусмотренных пунктом 7.3.1. настоящего Положения.

7.5. В целях соблюдения действующего законодательства Российской Федерации и обеспечения положений трудового договора возможна передача:

а) документов, содержащих сведения о доходах и налогах на доходы физических лиц, сведений о пенсионных накоплениях физических лиц в соответствии с действующим законодательством Российской Федерации – в федеральные органы исполнительной власти;

б) персональных данных для осуществления выдачи заработной платы или других доходов работника – в уполномоченные банковские организации;

в) персональных данных для содействия работникам в трудоустройстве, обучении, повышении их квалификации, переподготовке, проведения аттестации на квалификационную категорию, получение государственных наград и иных форм поощрения – в представительные органы власти, уполномоченные федеральные и региональные органы исполнительной власти.

Передача указанных сведений и документов осуществляется с согласия работника. Согласие работника оформляется письменно в виде отдельного документа. После получения согласия работника дальнейшая передача указанных сведений и документов, дополнительного письменного согласия работника не требует и в «Журнал учета запросов персональных данных работника по запросам третьих лиц» не фиксируется.

Учреждение обеспечивает ведение Журнала учета выданных персональных данных пациентов и работников по запросам третьих лиц, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

7.6. В случае, если лицо, обратившееся с запросом, не уполномочено действующим законодательством Российской Федерации на получение персональных данных пациента или работника, либо отсутствует письменное согласие пациента или работника на передачу его персональных данных, Учреждение обязано отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится в Учреждении.

8. Общедоступные источники персональных данных пациентов и работников.

8.1. Включение персональных данных пациента в общедоступные источники персональных данных возможно только при наличии его письменного согласия.

8.2. В целях информационного обеспечения работодателем могут создаваться общедоступные источники персональных данных работников (в том числе справочники, адресные книги, информационные стенды для потребителей услуг, оказываемых работодателем). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, иные персональные данные, предоставленные работником.

8.3. При обезличивании персональных данных согласие пациента или работника на включение персональных данных в общедоступные источники персональных данных не требуется.

8.4. Сведения о пациентах или работниках могут быть исключены из общедоступных источников персональных данных по требованию самого пациента или работника, либо по решению суда или иных уполномоченных государственных органов.

9. Права и обязанности пациента и работника в области защиты его персональных данных.

9.1. В целях обеспечения защиты персональных данных, хранящихся у Учреждения, пациенты имеют право на:

9.1.1. Полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;

9.1.2. Свободный доступ к своим персональным данным.

9.1.3. Пациент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных Учреждением;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые Учреждением способы обработки персональных данных;

г) наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона «О персональных данных»;

д) сроки обработки персональных данных, в том числе сроки их хранения;

е) порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством Российской Федерации;

ж) информацию об осуществленной или предполагаемой трансграничной передаче данных;

з) наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

и) иные сведения, предусмотренные федеральным законом «О персональных данных» или иными федеральными законами.

9.2. Сведения должны быть предоставлены пациенту Учреждением в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются пациенту или его представителю Учреждением при обращении либо при получении запроса пациента или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность пациента или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие пациента в отношениях с Учреждением (номер договора, дата заключения договора, устное словесное обращение или иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись пациента или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с действующим законодательством Российской Федерации.

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления пациенту по его запросу, пациент вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения 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 действующим законодательством Российской Федерации, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Пациент вправе требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать необходимые законом меры по защите своих прав.

9.3. В случае выявления неправомерной обработки персональных данных при обращении пациента или его представителя либо по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения)с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациента или третьих лиц.

9.4. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных пациентом или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом по поручению Учреждения) в течение семи дней со дня представления таких сведений и снять блокирование персональных данных.

9.5. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим на основании поручения Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить пациента или его представителя либо уполномоченный орган по защите прав субъектов персональных данных.

9.6. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент, иным соглашением между Учреждением и пациентом, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных федеральным законом «О персональных данных» или иными федеральными законами.

9.7. В случае отзыва пациентом согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующимпо поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и пациентом, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законом «О персональных данных» или иными федеральными законами.

9.8. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральным законодательством.

9.9. Для своевременной и полной реализации своих прав, пациент обязан предоставлять Учреждению достоверные и полные персональные данные.

9.10. Работник обязан:

9.10.1. При приеме на работу предоставить работодателю свои полные и достоверные персональные данные.

9.10.2. Для своевременной и полной реализации своих трудовых, пенсионных и иных прав работник обязуется поставить в известность работодателя об изменении персональных данных, обрабатываемых работодателем в связи с трудовыми отношениями, в том числе изменении фамилии, имени, отчества, паспортных данных, о получении образования, квалификации, получении инвалидности и иных медицинских заключений, препятствующих выполнению своих должностных обязанностей, и прочих данных с предоставлением подтверждающих документов.

9.11. В целях обеспечения защиты персональных данных работник имеет право на:

9.11.1. Полную информацию о хранящихся у работодателя его персональных данных.

9.11.2. Свободный бесплатный доступ к своим персональным данным, включая право на получении копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных действующим законодательством Российской Федерации. Выдача документов, содержащих персональные данные работников, осуществляется в соответствии со статьей 62 Трудового кодекса Российской Федерации, статьей 14 федерального закона «О персональных данных» с соблюдением следующей процедуры:

- работник должен предоставить заявление о выдаче того или иного документа на имя главного врача Учреждения;

- заверенная копия документа (в количестве экземпляров, необходимом работнику) выдается работнику в установленные действующим законодательством Российской Федерации сроки;

- в Журнал учета выданных персональных данных вносится соответствующая запись.

9.11.3. Требовать исключение или исправление неверных или неполных персональных данных, а также данных, обработанных с нарушениями. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

9.11.4. Требовать об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

9.11.5. Обжаловать в суд любые неправомерные действия или бездействия работодателя приобработку и защите его персональных данных.

9.11.6. Реализовывать иные права, предусмотренные действующим законодательством Российской Федерации.

9.12. Работодатель обязан:

9.12.1. Предоставить работнику, по его просьбе информацию о наличии у него персональных данных владельца, цели их обработки, способ обработки, разъяснить юридические последствия отказа работника от их предоставления в случае, если такая обязанность предусмотрена действующим законодательством Российской Федерации.

9.12.2. По письменному заявлению работника не позднее трех рабочих дней со дня его подачи бесплатно выдавать работнику копии документов, связанных с работой.

9.12.3. Устранять выявленные недостоверные персональные данные в случаях и порядке, предусмотренных действующим законодательством Российской Федерации.

9.12.4. Принимать возможные меры по обеспечению безопасности персональных данных работников при их обработке.

9.13. Работодатель имеет права:

9.13.1. Требовать от работника предоставления персональных данных и документов, их подтверждающих, в случаях, предусмотренных действующим законодательством Российской Федерации.

9.13.2. Иные права, предусмотренные действующим законодательством Российской Федерации.

10. Право на обжалование действий или бездействия Учреждения.

10.1. Если пациент, его законный представитель или работник Учреждения считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований федерального закона «О персональных данных» или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

10.2. Пациент и работник Учреждения имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебной порядке. Моральный вред, причиненный пациенту или работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных действующим законодательством Российской Федерации, а также требований к защите персональных данных, установленных действующим законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

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

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента и работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

11.2. Работники Учреждения, допущенные к обработке персональных данных пациентов и работников, за разглашение полученной в ходе своей трудовой деятельности информации, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

12. Заключительные положения.

12.1. Настоящее Положение вступает в силу с момента (даты) его утверждения.

12.2. Настоящее положение распространяется на всех пациентов и работников Учреждения.

Пациенты Учреждения, а также их законные представители имеют право, ознакомится с настоящим Положением.

Работники Учреждения подлежат ознакомлению с данным документом в порядке, предусмотренном приказом главного врача Учреждения под личную подпись.

12.3. В обязанности работников, осуществляющих первичный сбор персональных данных пациента, входит получение согласия пациента на обработку его персональных данных под личную подпись.

12.4. В обязанности работодателя входит ознакомление всех работников с настоящим Положением и лиц, принимаемых на работу до подписания трудового договора, под личную подпись.