

**Государственное бюджетное учреждение здравоохранения
Самарской области «Тольяттинская городская больница № 4»**

ПРИКАЗ

30.10.2020 № 314

г.Тольятти, Самарская область

О защите информации

В целях обеспечения защиты персональных данных, а так же в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», в редакции (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ, от 05.04.2013 № 43-ФЗ, от 23.07.2013 № 205-ФЗ, от 21.12.2013 № 363-ФЗ, от 04.06.2014 № 142-ФЗ, от 21.07.2014 № 216-ФЗ, от 21.07.2014 № 242-ФЗ), и Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

1.1. Положение о защите персональных данных пациентов ГБУЗ СО «ТГБ № 4» (приложение № 1).

1.2. перечень должностей, имеющих доступ к персональным данным пациентов (законных представителей) (приложение № 2).

1.3. форму документа «Согласие пациента (законного представителя) на обработку его персональных данных» (приложение № 3).

1.4. форму документа «Обязательство о неразглашении конфиденциальной информации (персональных данных)» (приложение № 4).

2. Назначить ответственным лицом за организацию деятельности по защите персональных данных заместителя главного врача по медицинской части Скачкову С.Н., в структурных подразделениях учреждения – руководителей структурными подразделениями.

3. Назначить ответственным лицом за контролем по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных начальника Бюро АСУ Митрофанова Г.Г.

4. Заместителю главного врача по медицинской части Скачковой С.Н., начальнику бюро АСУ Митрофанову Г.Г. ознакомить под роспись руководителей структурных подразделений с действующим законодательством Российской Федерации о персональных данных и организационно-распорядительной документацией, определяющими правила обработки персональных данных и требования по защите персональных данных, настоящим приказом.

Срок до 30.11.2020

5. Руководителям структурных подразделений довести до сведения своих сотрудников под роспись Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», настоящий приказ.

Срок до 30.11.2020

6. Заведующим структурными подразделениями - врачам – специалистам:

6.1. Организовать получение от пациентов (законных представителей) при обращении за медицинской помощью письменного согласия на обработку персональных данных пациента/персональных данных пациента и законного представителя в соответствии с формой документа (приложение № 3);

6.2. Обеспечить хранение письменного согласия на обработку персональных данных пациента/персональных данных пациента и законного представителя: в медицинской карте стационарного больного, в травматологической карте, в журналах регистрации и др.

Срок: постоянно

7. Начальнику отдела кадров Корноуховой Т.В.:

7.1. При приеме на работу (до подписания трудового договора) на должности, указанные в приложении № 2 настоящего приказа, получать письменное обязательство о неразглашении конфиденциальной информации (персональных данных) в соответствии с формой документа (приложение № 4).

Срок: постоянно

7.2. При получении письменного обязательства о неразглашении конфиденциальной информации (персональных данных) (приложение № 4) предупреждать сотрудников об ответственности за разглашение и (или) утрату информации (персональных данных).

Срок: постоянно

8. Начальнику бюро АСУ Митрофанову Г.Г. разместить Положение о защите персональных данных пациентов ГБУЗ СО «ТГБ № 4» (приложение № 1) в информационно - телекоммуникационной сети «Интернет» на официальном сайте учреждения.

Срок до 30.11.2020

9. Считать утратившими силу приказ ГБУЗ СО «ТГБ № 4» от 12.09.2018 № 199 «О защите информации».

10. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач



С.Н. Тетюшкин

**ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ
ГБУЗ СО «ТГБ № 4»**

1. Общая часть

1.1 Настоящее Положение определяет порядок создания, обработки и защиты персональных данных пациентов ГБУЗ СО «ТГБ № 4» (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);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ);
- Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее – Закон № 323-ФЗ);
- Другие нормативные правовые акты Российской Федерации.

1.3 Целью настоящего Положения является определение порядка обработки персональных данных пациентов Учреждения-оператора, согласно Перечню персональных данных, указанных в разделе 3 настоящего Положения, 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, имеющих доступ к персональным данным пациентов, 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 негосударственной (служебной, профессиональной) тайны.

2. Основные понятия, используемые в настоящем Положении

Для целей настоящего Положения применяются следующие термины и определения:

Оператор – Учреждение-оператор 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 медицинской помощи, либо состоящие в иных гражданско-правовых отношениях с Учреждением-оператором по вопросам получения медицинских услуг.

Врачебная тайна – сведения о факте обращения пациента (субъекта персональных данных) за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском 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 пациенту (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 – обязательное для соблюдения должностным лицом Учреждения-оператора, иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия пациента (субъекта персональных данных) или наличия иного законного основания.

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 пациента (субъекта персональных данных) или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Лица, допущенные к персональным данным – работники Учреждения-оператора, которые в силу своих должностных обязанностей либо занимаемой должности осуществляют обработку персональных данных, либо совершающие действия (операции) с персональными данными.

3. Перечень персональных данных

3.1. В состав обрабатываемых в Учреждении-операторе персональных данных пациентов могут входить:

- Фамилия, имя, отчество;
- Пол;
- Дата и место рождения;
- Адрес места проживания и регистрации;
- Документ, удостоверяющий личность;
- Реквизиты полиса ОМС (ДМС);
- Данные о состоянии здоровья (медицинская карта стационарного больного, справки, результаты исследований, другие документы, содержащие персональные данные), случаях обращения за медицинской помощью;

- Другая информация, необходимая для правильного проведения медицинских исследований;

- Данные о месте работы и занимаемой должности;

- Другая информация, несущая персональные данные и не запрещенная на территории РФ.

3.2. Учреждение-оператор осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинской помощи, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

4. Лица, допущенные к персональным данным

3.1. Доступ к персональным данным пациентов имеют сотрудники Учреждения-оператора, непосредственно использующие эти данные в рамках выполнения своих должностных обязанностей.

Перечень должностей, имеющих доступ к персональным данным пациентов, определяется приказом главного врача.

5. Случаи, когда для обработки персональных данных не требуется согласия субъекта персональных данных

5.1. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.

5.2. Обработка персональных данных пациента (субъекта персональных данных) без получения его согласия осуществляется в следующих случаях:

1) для защиты жизни, здоровья или иных жизненно важных интересов пациента (субъекта персональных данных) либо жизни, здоровья или иных жизненно важных интересов других лиц, если получение согласия пациента (субъекта персональных данных) невозможно;

2) при поступлении запроса органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, запроса органов прокуратуры в связи с осуществлением ими прокурорского надзора, запроса органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

3) для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) в других случаях, предусмотренных федеральными законами.

6. Общие принципы и условия обработки персональных данных пациентов

6.1. Обработка персональных данных пациента осуществляется на основе принципов:

1) Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

3) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4) Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5) 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.

б) 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-оператор должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7) 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 Законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент (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 федеральными законами.

6.2. В целях обеспечения прав и свобод человека и гражданина Учреждение-оператор и его представители при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

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 законодательством Российской Федерации.

2) Все персональные данные пациента следует получать у него самого или у его полномочного представителя. 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) При определении объема и содержания обрабатываемых персональных данных пациента, Учреждение-оператор должно руководствоваться Конституцией Российской Федерации, Законом № 323-ФЗ, законодательством РФ в сфере защиты персональных данных и обработки информации, Уставом Учреждения-оператора и иными локальными нормативными актами в области защиты персональных данных.

4) Учреждение-оператор не имеет права получать и обрабатывать персональные данные пациента, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Законом № 152-ФЗ.

5) Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении пациента или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Законом № 152-ФЗ.

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

7) Учреждение-оператор обязано разъяснить пациенту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты пациентом своих прав и законных интересов.

8) Учреждение-оператор обязано рассмотреть возражение в течение тридцати дней со дня его получения и уведомить пациента о результатах рассмотрения такого возражения.

9) Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Учреждением-оператором за счет своих средств, в порядке, установленном федеральными законами и другими нормативными документами.

6.3. Учреждение-оператор вправе поручить обработку персональных данных другому лицу с согласия пациента, если иное не предусмотрено Законом № 152-ФЗ, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение Учреждения-оператора). Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом № 152-ФЗ. В поручении Учреждения-оператора 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 Закона № 152-ФЗ.

6.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, не обязано получать согласие пациента на обработку его персональных данных.

6.5. В случае если Учреждение-оператор поручает обработку персональных данных другому лицу, ответственность перед пациентом за действия указанного лица несет Учреждение-оператор. Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, несет ответственность перед Учреждением-оператором.

7. Получение персональных данных пациента

7.1. Получение персональных данных преимущественно осуществляется путем представления их самим пациентом, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством РФ.

В случаях, предусмотренных действующим законодательством, обработка персональных данных осуществляется только с согласия пациента в письменной форме. Равнозначным содержащему собственноручную подпись пациента согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Законом № 152-ФЗ электронной подписью. Согласие пациента в письменной форме на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя пациента (субъекта персональных данных), номер основного документа, удостоверяющего его 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 пациента);

3) наименование и адрес Учреждения-оператора, получающего согласие пациента;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие пациента;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения-оператора, если обработка будет поручена такому лицу;

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

8) срок, в течение которого действует согласие пациента, а также способ его отзыва, если иное не установлено федеральными законами;

9) подпись пациента.

6.6. В случае недееспособности пациента, не достижения пациентом возраста 15 лет, в других случаях согласие на обработку его персональных данных дает в письменной форме его

законный представитель.

7.2. В случае необходимости проверки персональных данных пациента Учреждение-оператор заблаговременно должно сообщить об этом пациенту, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение. Учреждение-оператор при обработке персональных данных пациентов 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.

8. Хранение и использование персональных данных пациентов

8.1. Информация персонального характера пациента хранится и обрабатывается с соблюдением требований действующего законодательства РФ о защите персональных данных.

8.2. Порядок хранения документов, содержащих персональные данные пациентов осуществлять в соответствии с:

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

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

8.3. Обработка персональных данных пациентов осуществляется смешанным путем:

- неавтоматизированным способом обработки персональных данных;
- автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

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

8.5. Хранение содержащие персональные данные пациентов и окончанных производством документов, содержащих персональные данные пациентов, осуществляется во внутренних помещениях Учреждения-оператора, а также в помещениях Учреждения-оператора, предназначенных для хранения отработанной документации.

8.6. Возможна передача персональных данных пациентов по внутренней сети организации с использованием технических и программных средств защиты информации, с доступом только для сотрудников Учреждения-оператора, допущенных к работе с персональными данными пациентов и только в объеме, необходимом данным сотрудникам для выполнения своих должностных обязанностей.

8.7. Хранение персональных данных пациентов 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, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

8.8. Учреждение-оператор обеспечивает ограничение доступа к персональным данным пациентов лицам, не уполномоченным федеральными законами, либо Учреждением-оператором для получения соответствующих сведений.

8.9. Доступ к персональным данным пациентов имеют только сотрудниками Учреждения-оператора, подписавшие обязательство о неразглашение конфиденциальной информации. Персональные данные выдаются, в объеме, необходимом для выполнения своих должностных обязанностей.

8.10. Ответственными за организацию и осуществление хранения персональных данных пациентов Учреждения-оператора являются руководители структурных подразделений.

8.11. Контроль за обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями законодательства РФ возлагается на начальника бюро АСУ.

9. Защита персональных данных пациентов

9.1. Учреждение-оператор при обработке персональных данных пациентов 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.

9.2. Обеспечение безопасности персональных данных пациентов достигается, в частности:

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

2) 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;

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

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

5) учетом машинных носителей персональных данных;

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

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

8) 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;

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

9.3. Для обеспечения безопасности персональных данных пациентов при неавтоматизированной обработке предпринимаются следующие меры:

9.3.1. Определяются места хранения персональных данных (согласно настоящему Положению), которые оснащаются следующими средствами защиты:

- В кабинетах, где осуществляется хранение документов, содержащих персональные данные пациентов, имеются сейфы, шкафы, стеллажи, тумбы.

- Дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные пациентов, оборудованы замками и системой пожарной сигнализации.

9.3.2. Все действия при неавтоматизированной обработке персональных данных пациентов осуществляются только должностными лицами Учреждения-оператора, допущенными к персональным данным, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

9.3.3. 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:

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;

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.

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, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить отдельную 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.

9.3.4. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9.4. Для обеспечения безопасности персональных данных пациентов при автоматизированной обработке предпринимаются следующие меры:

9.4.1. Все действия при автоматизированной обработке персональных данных пациентов осуществляются только должностными лицами, допущенными к персональным данным, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

9.4.2. Персональные компьютеры, имеющие доступ к базам хранения персональных данных пациентов, защищены паролями доступа. Пароли устанавливаются сотрудниками бюро АСУ и сообщаются индивидуально сотруднику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов на данном ПК.

9.4.3. Иные меры, предусмотренные нормативными правовыми актами по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

9.4.4. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законодательством РФ.

10. Передача персональных данных пациентов третьим лицам

10.1. Передача персональных данных пациентов третьим лицам осуществляется Учреждением-оператором только с письменного согласия пациента, с подтверждающей визой руководителя (заместителя руководителя по медицинской части) Учреждения-оператора, за исключением случаев, если:

1) передача необходима для защиты жизни и здоровья пациента, либо других лиц, и получение его согласия невозможно;

2) в целях обследования и лечения пациента, не способного из-за своего состояния выразить свою волю;

3) в случаях, предусмотренных статьей 13 Закона № 323-ФЗ, в том числе по запросу

органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, прокуратуры в связи с осуществлением ими прокурорского надзора и т.д.;

4) в случае оказания помощи несовершеннолетнему в возрасте до 15 лет, для информирования его родителей или законных представителей;

5) при наличии оснований, позволяющих полагать, что права и интересы пациента могут быть нарушены противоправными действиями других лиц;

б) в иных случаях, прямо предусмотренных федеральными законами.

Лица, которым в установленном Законом № 152-ФЗ порядке переданы сведения, составляющие персональные данные пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность за разглашение в соответствии с законодательством Российской Федерации.

10.2. Передача персональных данных пациента третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой руководителя (заместителя руководителя по медицинской части) Учреждения-оператора при условии соблюдения требований, предусмотренных п. 7.1 настоящего Положения.

В случае если лицо, обратившееся с запросом, не уполномочено федеральными законами на получение персональных данных пациента, либо отсутствует письменное согласие пациента на передачу его персональных данных, Учреждение-оператор 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 у Учреждения-оператора.

11. Общедоступные источники персональных данных пациентов

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

11.2. При обезличивании персональных данных согласие пациента на включение персональных данных в общедоступные источники персональных данных не требуется.

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

12. Права и обязанности пациента в области защиты его персональных данных

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

- полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;

- свободный доступ к своим персональным данным.

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

1) подтверждение факта обработки персональных данных Учреждением-оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Учреждением-оператором способы обработки персональных данных;

4) наименование и место нахождения Учреждения-оператора, сведения о лицах (за исключением сотрудников Учреждения-оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением-оператором или на основании Закона № 152-ФЗ;

5) обрабатываемые персональные данные, относящиеся к соответствующему пациенту, источник их получения, если иной порядок представления таких данных не предусмотрен Законом № 152-ФЗ;

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

7) порядок осуществления пациентом прав, предусмотренных Законом № 152-ФЗ;

8) информацию об осуществленной или о предполагаемой трансграничной передаче

данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения-оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Законом № 152-ФЗ или другими федеральными законами.

Сведения должны быть предоставлены пациенту Учреждением-оператором 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 законному представителю Учреждением-оператором при обращении, либо при получении запроса пациента или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность пациента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие пациента в отношениях с Учреждением-оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением-оператором, подпись пациента или его законного представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с 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-оператору 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 федеральными законами, принятым в соответствии с ними нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является пациент.

Пациент вправе требовать от Учреждения-оператора 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 предусмотренные Законом № 152-ФЗ меры по защите своих прав.

12.2. В случае выявления неправомерной обработки персональных данных при обращении пациента или его законного представителя, либо по запросу пациента или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Учреждение-оператор обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому пациенту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение-оператор обязано осуществить блокирование персональных данных, относящихся к этому пациенту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) 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.

12.3. В случае подтверждения факта неточности персональных данных Учреждение-оператор на основании сведений, представленных пациентом или его законным представителем, либо уполномоченным органом по защите прав пациента, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в течение семи рабочих дней со дня представления

таких сведений и снять блокирование персональных данных.

12.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением-оператором (или лицом, действующим по поручению Учреждения-оператора), Учреждение-оператор 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-оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение-оператор в срок, не превышающий десяти рабочих 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-оператор обязано уведомить пациента или его законного представителя, а в случае, если обращение пациента или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав пациента, также указанный орган.

12.5. В случае достижения цели обработки персональных данных Учреждение-оператор обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) 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-оператором и пациентом, либо если Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных Законом № 152-ФЗ или другими федеральными законами.

12.6. В случае отзыва пациентом согласия на обработку его персональных данных Учреждение-оператор обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) 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, действующим по поручению Учреждения-оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент, иным соглашением между Учреждением-оператором и пациентом, либо если Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных Законом № 152-ФЗ или другими федеральными законами.

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

12.8. Для своевременной и полной реализации своих прав, пациент обязан предоставить Учреждению-оператору достоверные персональные данные.

13. Право на обжалование действий или бездействия Учреждения-оператора

13.1. Если пациент или его законный представитель считает, что Учреждение-оператор осуществляет обработку его персональных данных с нарушением требований Закона № 152-ФЗ или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Учреждения-оператора в уполномоченный орган по защите прав субъектов персональных данных (Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи) или в судебном порядке.

13.2. Пациент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Моральный вред, причиненный пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

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

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

15. Заключительные положения

15.1. Настоящее Положение вступает в силу с даты его утверждения.

15.2. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании приказа руководителя Учреждения-оператора.

15.3. Настоящее Положение распространяется на всех пациентов Учреждения-оператора, а также сотрудников Учреждения-оператора, имеющих доступ и осуществляющих перечень действий с персональными данными пациентов.

Пациенты Учреждения-оператора, а также их законные представители имеют право ознакомиться с настоящим Положением.

Сотрудники Учреждения-оператора подлежат ознакомлению с настоящим Положением в порядке, предусмотренном приказом руководителя Учреждения-оператора.

Перечень должностей, имеющих доступ
к обработке персональных данных пациента (законного представителя)

Главный врач
Заместитель главного врача по медицинской части
Заместитель главного врача по клинико-экспертной работе
Заместитель главного врача по хозяйственным вопросам
Заместитель главного врача по экономическим вопросам
Заместитель главного врача по гражданской обороне и мобилизационной работе
Главная медицинская сестра
Врач-эпидемиолог
Врач клинический фармаколог
Медицинский психолог
Заведующий аптекой
Фармацевт
Заведующий структурным подразделением - врач – специалист
Врач-специалист
Старшая медицинская сестра
Медицинская сестра
Медицинская сестра диетическая
Медицинская сестра палатная
Медицинская сестра процедурной
Медицинская сестра перевязочной
Операционная медицинская сестра
Медицинская сестра - анестезист
Медицинская сестра приемного отделения
Медицинская сестра приемного отделения (наркопост)
Старшая операционная медицинская сестра
Медицинская сестра по физиотерапии
Медицинская сестра по массажу
Инструктор по лечебной физкультуре
Рентгенолаборант
Младшая медицинская сестра по уходу за больным
Биолог
Лаборант
Фельдшер-лаборант
Медицинский лабораторный техник
Медицинский технолог
Медицинский регистратор
Медицинский статистик
Начальник юридического отдела
Ведущий юрисконсульт
Специалист по закупкам
Специалист по охране труда
Начальник отдела кадров
Специалист по кадрам
Начальник технического отдела

Главный бухгалтер
Заместитель главного бухгалтера
Бухгалтер
Начальник планово-экономического отдела
Экономист
Кассир
Курьер
Начальник бюро АСУ
Инженер-программист
Инженер - электроник
Архивариус
Секретарь руководителя
Делопроизводитель
Менеджер
Оператор электронно-вычислительных и вычислительных машин
Инженер

**СОГЛАСИЕ ПАЦИЕНТА (ЗАКОННОГО ПРЕДСТАВИТЕЛЯ)
НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ**Я, _____
(ФИО пациента полностью)Паспорт (серия и номер) _____ выдан (дата) _____
название выдавшего органа _____,

Проживающий по адресу _____

По месту регистрации _____
или законный представитель пациента _____

(ФИО законного представителя полностью)

Паспорт (серия и номер) _____ выдан (дата) _____
название выдавшего органа _____,Доверенность (иной документ), подтверждающий полномочия _____
(Реквизиты доверенности (иного документа))

Проживающий по адресу _____

По месту регистрации _____
выступающий представителем _____

(ФИО пациента полностью)

в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных» подтверждаю свое согласие на автоматизированную, а также без использования средств автоматизации Государственным бюджетным учреждением здравоохранения Самарской области «Тольяттинская городская больница № 4» (далее – Оператор) моих персональных данных/моих персональных данных и моего представляемого, включающих фамилию, имя, отчество, пол, дату и место рождения, адрес места проживания и регистрации, номера контактных телефонов, адрес электронной почты, гражданство, серию и номер документа, удостоверяющего личность, реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), данные об образовании, профессии, должности и месте работы или учебы, сведения о социальном статусе, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью, в целях установления диагноза и оказания медицинских услуг, других персональных данных в соответствии с федеральными законами и иными нормативными правовыми актами РФ.

В процессе оказания Оператором мне/моему представляемому медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные/данные моего представляемого, содержащие сведения, составляющие врачебную тайну, другим работникам Оператора в интересах моего/его обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными/персональными данными моими и моего представляемого, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Оператор вправе обрабатывать мои персональные данные/персональные данные моего представляемого посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов).

Учреждение-Оператор имеет право передачи моих персональных данных/персональных данных моего представляемого при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с использованием машинных носителей или по каналам связи.

Передача моих персональных данных/персональных данных моих и моего представляемого иным лицам или в иных случаях может осуществляться только с моего письменного согласия.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет (для стационара), пять лет (для поликлиники).

Настоящее согласие дано мной «_____» _____ 20__ г. и действует бессрочно.

Я оставляю за собой право отозвать свое согласие/согласие моего представляемого посредством составления соответствующего письменного документа.

Подпись пациента/законного представителя _____

«_____» _____ 20__ г.

**ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации (персональных данных)**

Я, _____
(ФИО сотрудника)

(должность, наименование структурного подразделения)

предупрежден(а), что в соответствии с должностной инструкцией мне будет предоставлен допуск к конфиденциальной информации (персональным данным пациентов, сотрудников). В период трудовой деятельности в ГБУЗ СО «ТГБ № 4» и после увольнения добровольно принимаю на себя обязательства:

1. Не разглашать, не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
3. Не использовать конфиденциальные сведения с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

(ФИО)
« _____ » _____ 20__ г.

(подпись)