

СОГЛАСОВАНО
Председатель
профсоюзного комитета
ГАУЗ «АМИАЦ»

УТВЕРЖДАЮ
Главный врач
ГАУЗ «АМИАЦ»


/ И.Г. Якимова /


/ В.З. Мухутдинова /

Протокол заседания профкома
№ _____ от _____ 2014 г.

«05» апреля 2014 г.

**ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ
ГАУЗ «АМИАЦ»**

1 Общая часть

1.1 Настоящее Положение определяет порядок создания, обработки и защиты персональных данных работников ГАУЗ «АМИАЦ» (далее – Учреждение-оператор).

1.2 Основанием для разработки данного локального нормативного акта являются:

- Конституция РФ от 12 декабря 1993 г. (ст. ст. 2, 17-24, 41);
- глава 14 (ст. 86-90) Трудового кодекса РФ;
- часть 1 и 2, часть 4 Гражданского кодекса РФ;
- Указ Президента РФ от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Федеральный закон от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 03 ноября 2006 г. № 174-ФЗ «Об автономных учреждениях»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или

муниципальными органами»;

- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Регламентирующие документы ФСТЭК России об обеспечении безопасности персональных данных:

- Приказ ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008 г.);

- Устав ГАУЗ «АМИАЦ» утвержден Первым заместителем министра земельных и имущественных отношений Республики Татарстан (Распоряжение № 3718-р от 21 декабря 2011 г.), согласовано с Министром здравоохранения Республики Татарстан (Приказ № ____ от «__» _____ 2011 г.);

- Приказ главного врача ГАУЗ «АМИАЦ» № ____ от «__» _____ 2014 г. «О защите персональных данных работников».

1.3 Целью настоящего Положения является определение порядка обработки персональных данных лиц, работающих по трудовым договорам и гражданско-правовым договорам (далее - работников) Учреждения-оператора, согласно Перечня персональных данных, утвержденного Приказом главного врача Учреждения-оператора (Приложение № 1 к настоящему Положению); обеспечение защиты прав и свобод работников, при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

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.

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

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

Документы, содержащие персональные данные работника - документы, которые работник предоставляет Учреждению-оператору (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.

Обработка персональных данных 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 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 работников

3.1 Обработка персональных данных 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.

6) 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 Федеральным законом №152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством.

3.2 В целях обеспечения прав и свобод человека и гражданина, работодатель и его представители при обработке персональных данных работников обязаны соблюдать следующие общие требования:

1) 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 № 152-ФЗ «О персональных данных», оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, содействия работникам в трудоустройстве, обучении, повышении квалификации и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества работодателя.

2) Все персональные данные работника работодатель должен получать у него самого. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

3) При определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными Федеральными законами.

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

5) Учреждение-оператор не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законодательством.

6) Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении работника или иным образом затрагивающих его права и законные интересы, за исключением

случаев, предусмотренных Федеральным законом № 152-ФЗ.

7) Решение, порождающее юридические последствия в отношении работника 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 работника или в случаях, предусмотренных Федеральным законодательством, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

8) Учреждение-оператор обязано разъяснить работнику 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 субъектом работником своих прав и законных интересов.

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

10) Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена Учреждением-оператором за счет своих средств, в порядке, установленном Федеральным законодательством и другими нормативными документами.

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

4 Получение персональных данных работников

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

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

1) фамилию, имя, отчество, адрес 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 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 субъекта персональных данных);

3) наименование и адрес оператора (ГАУЗ «АМИАЦ»), получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

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

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 субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;

9) подпись субъекта персональных данных.

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

4.2 В случае необходимости проверки персональных данных работника работодатель должен заблаговременно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.3 Обработка персональных данных работника не требует получения соответствующего согласия в следующих случаях:

1) Если объем обрабатываемых работодателем персональных данных не превышает установленные перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством.

2) Обязанность по обработке, в том числе опубликованию и размещению персональных данных работников в сети Интернет, предусмотрена законодательством Российской Федерации.

3) Обработка персональных данных близких родственников работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление социальных выплат). В иных случаях, получение согласия

близких родственников работника является обязательным условием обработки их персональных данных.

4) Обработка специальных категорий персональных данных работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Федерального закона «О персональных данных» в рамках трудового законодательства.

5) При передаче персональных данных работника третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

6) При передаче его персональных данных в случаях, связанных с выполнением им должностных обязанностей, в том числе, при его командировании (в соответствии с Правилами оказания гостиничных услуг в Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 25 апреля 1997 г. № 490, нормативными правовыми актами в сфере транспортной безопасности).

7) В случаях передачи работодателем персональных данных работников в налоговые органы, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством Российской Федерации.

8) При мотивированных запросах от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, работодатель обязан получить согласие работника на предоставление его персональных данных и предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

9) Передача персональных данных работника кредитным организациям, открывающим и обслуживающим платежные карты для начисления заработной платы, осуществляется без его согласия в следующих случаях:

- договор на выпуск банковской карты заключался напрямую с работником, и в тексте которого предусмотрены положения,

предусматривающие передачу работодателем персональных данных работника;

- наличие у работодателя доверенности на представление интересов работника при заключении договора с кредитной организацией на выпуск банковской карты и ее последующем обслуживании;

- соответствующая форма и система оплаты труда прописана в коллективном договоре (ст. 41 Трудового кодекса РФ).

10) Обработка персональных данных работника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя, при условии, что организация пропускного режима осуществляется работодателем самостоятельно либо если указанная обработка соответствует порядку, предусмотренному коллективным договором, локальными актами работодателя, принятыми в соответствии с ст. 372 Трудового кодекса РФ.

5 Хранение и использование персональных данных работников

5.1 Информация персонального характера работника хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

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

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

- Унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными Постановлением Госкомстата России от 05 января 2004 г. № 1;

- 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»;

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

5.3 Обработка персональных данных работников осуществляется смешанным путем:

- неавтоматизированным способом обработки персональных данных;

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

5.4 Персональные данные работников хранятся на бумажных

носителях и в электронном виде.

5.5 Личные дела, трудовые книжки, личные медицинские книжки, а также документы, содержащие персональные данные работников Учреждения-оператора, хранятся в кабинетах № 1, № 8, № 12, №13, № 15.

Ответственные лица за хранение документов, содержащих персональные данные работников, назначены Приказом главного врача Учреждения-оператора.

5.6 Хранение оконченных производством документов, содержащих персональные данные работников Учреждения-оператора, осуществляется в помещении Учреждения-оператора, предназначенном для хранения отработанной документации.

Ответственные лица за хранение оконченных производством документов, содержащих персональные данные работников, назначены Приказом главного врача Учреждения-оператора.

5.7 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, 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 работников, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения, документы подлежат уничтожению в порядке, предусмотренном приказами по архивному делу.

5.8 Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным Федеральным законодательством, либо работодателем для получения соответствующих сведений.

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

Персональные данные работников в полном объеме выдаются только главному врачу, начальнику отдела кадров, специалисту по кадрам, заведущему бухгалтеру.

Иным должностным лицам работодателя, допущенным к работе с персональными данными работников, документы, содержащие персональные данные выдаются, в объеме, необходимом для выполнения своих должностных обязанностей.

Начальник отдела кадров, специалист по кадрам – единственные должностные лица, которые могут формировать личные дела, снимать копии с документов, делать выписки, составлять аналитические справки, и изымать

(заменять) документы, хранящиеся в личных делах работников. Передача данных прав и полномочий вышеуказанных лиц иным должностным лицам работодателя без специально оформленного Приказа главного врача Учреждения-оператора запрещается.

6 Защита персональных данных работников

6.1 Учреждение-оператор при обработке персональных данных 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 Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.3 Обеспечение безопасности персональных данных работников 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.

6.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона № 152 «О персональных данных».

6.5. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона № 152 «О персональных данных».

6.6. Для обеспечения безопасности персональных данных работника при неавтоматизированной обработке предпринимаются следующие меры:

6.6.1. Определяются места хранения персональных данных (согласно настоящего Положения), которые оснащаются следующими средствами защиты:

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

- Дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные работников, оборудованы замками и системами охранной (пультовой) и пожарной сигнализаций.

- Учреждение-оператор использует услуги вневедомственной охраны.

6.6.2. Все действия по неавтоматизированной обработке персональных данных работников осуществляются только должностными лицами, согласно Списка должностей, утвержденного Приказом главного врача Учреждения-оператора (Приложение № 3 к настоящему Положению), и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

В соответствии с п.п. «б» п. 1 Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211, перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных, указан в Списке должностей, утвержденном Приказом главного врача Учреждения-оператора (Приложение № 3 к настоящему Положению).

6.6.3. 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 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.

6.6.4 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».

6.7 Для обеспечения безопасности персональных данных работника при автоматизированной обработке предпринимаются следующие меры:

6.7.1 Все действия при автоматизированной обработке персональных данных работников осуществляются только должностными лицами, согласно Списка должностей, утвержденного Приказом главного врача Учреждения-оператора (Приложение № 2 к настоящему Положению), и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

В соответствии с п.п. «б» п. 1 Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211, перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных, указан в Списке должностей, утвержденном Приказом главного врача Учреждения-оператора (Приложение № 2 к настоящему Положению).

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

6.7.3 Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6.8 Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами по архивному делу, или продлевается на основании заключения экспертной комиссии Учреждения-оператора, если иное не определено законодательством РФ.

7 Передача персональных данных работников третьим лицам

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

7.1.1 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 законодательством РФ.

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

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

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

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

7.2 Передача персональных данных работника третьим лицам осуществляется на основании письменного заявления/запроса третьего лица с

разрешающей визой главного врача Учреждения-оператора и только с согласия работника, в отношении которого поступил такой запрос, за исключением случаев, прямо предусмотренных п. 7.1.1 настоящего Положения.

Учреждение-оператор обеспечивает ведение Журнала учета выданных персональных данных работников по запросам третьих лиц (Приложение № 4 к настоящему Положению), в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законодательством на получение персональных данных работника, либо отсутствует письменное согласие работника 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.

7.3 Получателями персональных данных работников Учреждения-оператора (внешний доступ) могут относиться организации, в т.ч. государственные учреждения, органы государственной власти, получающие персональные данные в объеме и в порядке, определенном действующим законодательством, а именно:

- налоговые органы;
- правоохранительные органы;
- судебные органы;
- органы статистики;
- военкоматы;
- органы социального страхования (медицинские страховые организации в соответствии с договором обязательного медицинского страхования работающих граждан);
- банковские организации;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- другие получатели, в том числе вышестоящие федеральные органы исполнительной власти (по подведомственности).

8 Общедоступные источники персональных данных работников

8.1 В целях информационного обеспечения работодателем могут создаваться общедоступные источники персональных данных (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.

8.2 При обезличивании персональных данных согласие работника на включение персональных данных в общедоступные источники персональных данных не требуется.

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

9 Права и обязанности работника и работодателя в области защиты персональных данных

9.1 Работник обязан:

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

9.1.2 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.

9.2 В целях обеспечения защиты персональных данных работник имеет право на:

9.2.1 Полную информацию о хранящихся у работодателя его персональных данных.

9.2.2 Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством РФ.

Выдача документов, содержащих персональные данные работников, осуществляется в соответствии со ст. 62 Трудового кодекса Российской Федерации, гл. 3 ст. 14 Федерального закона № 152-ФЗ с соблюдением следующей процедуры:

- заявление работника о выдаче того или иного документа на главного врача Учреждения-оператора (работодателя);
- выдача заверенной копии (в количестве экземпляров, необходимом работнику) заявленного документа либо справки о заявленном документе или сведениях, содержащихся в нем;
- внесение соответствующих записей в журнал учета выданной информации.

9.2.3 Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением. 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.

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

9.2.5 Обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

9.2.6 Иные права, предусмотренные действующим законодательством.

9.3 Работодатель обязан:

9.3.1 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 Федеральным законодательством.

9.3.2 По письменному заявлению работника не позднее 3-х рабочих дней со дня его подачи бесплатно выдавать работнику копии документов, связанных с работой.

9.3.3 Устранять выявленные недостоверные персональные данные в случаях и порядке, предусмотренном Федеральным законодательством.

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

9.4 Работодатель имеет право:

9.4.1 Требовать от работника предоставления персональных данных и документов, их подтверждающих, в случаях, предусмотренных Федеральным законодательством.

9.4.2 Иные права, предусмотренные действующим законодательством.

10 Право на обжалование действий или бездействия работодателя

10.1 Если работник считает, что работодатель осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, работник вправе обжаловать действия или бездействие работодателя 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.

10.2 Работник имеет право на защиту своих прав и законных интересов,

в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

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

11.1 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральным законодательством.

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

11.3 Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным 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.

12 Заключительные положения

12.1 Настоящее Положение утверждается и вводится в действие Приказом главного врача Учреждения-оператора.

12.2 Настоящее Положение вступает в силу с даты его утверждения и действует постоянно, до момента замены его новым, является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

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

12.4 Документы, определяющие политику в отношении обработки персональных данных работников, размещены на официальном сайте или информационном стенде Учреждения-оператора в течение 10 дней после их утверждения.

Приложение № 1 к
 Положению о защите
 персональных данных работников
 ГАУЗ «АМИАЦ»
 Утверждено Приказом № 11-А
 от «24» марта 2014 г.

ПЕРЕЧЕНЬ
категорий персональных данных работников,
обрабатываемых в ГАУЗ «АМИАЦ»

№ п/п	Основания для обработки	Содержание сведений	Категории субъектов	Срок хранения, условия прекращения обработки
1	Глава 14 Трудового кодекса РФ	фамилия, имя, отчество; паспортные данные; дата и место рождения; пол; гражданство; адрес места жительства; сведения о воинском учете; наименование высшего военного учреждения; воинское звание; семейное положение; сведения о составе семьи; сведения о детях; стаж работы; контактный номер телефона; сведения об образовании; профессия (специальность); наименование ВУЗа; сведения об аттестации; сведения о повышении квалификации; сведения о профессиональной переподготовке; сведения о наградах	Работники	По достижении целей обработки. 75 лет ЭПК*

№ п/п	Основания для обработки	Содержание сведений	Категории субъектов	Срок хранения, условия прекращения обработки
		(поощрениях), почетных званиях; сведения о социальных льготах; сведения о состоянии здоровья; сведения о заработной плате; сведения, содержащиеся в свидетельстве о постановке на учет в налоговом органе (ИНН); сведения, содержащиеся в страховом свидетельстве государственного пенсионного страхования (СНИЛС).		

* ЭПК означает, что часть таких документов может иметь научно-историческое значение и в установленном порядке должна передаваться в государственные, муниципальные архивы или храниться в организации (В соответствии с «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденным Приказом Минкультуры России от 25.08.2010 № 558)

Приложение № 2 к
Положению о защите
персональных данных работников
ГАУЗ «АМИАЦ»
Утверждено Приказом № 11-А
от «24» марта 2014 г.

Список
должностей работников ГАУЗ «АМИАЦ», уполномоченных на
автоматизированную обработку персональных данных работников

Административно-управленческий персонал

1. Начальник отдела кадров
2. Главный специалист по сестринскому делу
3. Ведущий инженер по охране труда и технике безопасности
4. Ведущий инженер по гражданской обороне и чрезвычайным ситуациям
5. Специалист по кадрам

Бухгалтерия

6. Ведущий бухгалтер

Отдел программного обеспечения

7. Ведущий программист

Медицинский персонал

8. Фельдшер

Приложение № 3 к
Положению о защите
персональных данных работников
ГАУЗ «АМИАЦ»
Утверждено Приказом № 11-А
от «24» марта 2014 г.

Список
должностей работников ГАУЗ «АМИАЦ», уполномоченных на
неавтоматизированную обработку персональных данных работников

Административно-управленческий персонал

1. Главный врач
2. Заместитель главного врача по экономическим вопросам
3. Заместитель главного врача
4. Начальник отдела кадров
5. Ведущий инженер по охране труда и технике безопасности
6. Ведущий инженер по гражданской обороне и чрезвычайным ситуациям
7. Ведущий юрисконсульт
8. Специалист по кадрам
9. Машинистка

Планово-экономический отдел

10. Главный специалист по экономике

Бухгалтерия

11. Главный бухгалтер
12. Ведущий бухгалтер

Отдел программного обеспечения

13. Ведущий программист

Административно-хозяйственный отдел

14. Начальник отдела материально-технического снабжения

Медицинский персонал

15. Начальник отдела учета и медицинской статистики

Приложение № 4 к
 Положению о защите
 персональных данных работников
 ГАУЗ «АМИАЦ»
 Утверждено Приказом № 11-А
 от «24» марта 2014 г.

**Журнал учета выданных персональных данных работников ГАУЗ «АМИАЦ» по запросам третьих лиц
 (органов прокуратуры, внутренних дел, службы судебных приставов, организаций и т.п.)**

№ п/п	Дата, № и реквизиты запроса	Дата и форма выдачи информации (письмо, факс и т.д.)	Ф.И.О. работника, в отношении которого поступил запрос	Цель обработки персональных данных	Краткое содержание информации	Сведения о согласии субъекта на предоставление персональных данных по данному запросу				Ф.И.О., должность, номер документа, удостоверяющего личность лица, получившего на руки ответ на запрос, подпись в получении
						Дата, № согласия работника, в отношении которого поступил запрос	Перечень персональных данных, на обработку которых дается согласие, срок его действия и порядок отзыва	Перечень действий с переданными персональными данными, на совершение которых дается согласие	Ф.И.О., должность работника, получающего согласие, подпись	
1	2	3	4	5	6	7	8	9	10	11