

Министерство здравоохранения
Астраханской области
Государственное бюджетное учреждение
здравоохранения Астраханской области
«Областная клиническая психиатрическая
больница»



УТВЕРЖДЕНО
приказом
главного врача ГБУЗ АО «ОКПБ»
№ 151 от 16.08.2013 г

ПОЛОЖЕНИЕ
о защите персональных данных

1. Общие положения

1.1. Положение о защите персональных данных (далее по тексту – Положение) определяет порядок сбора, обработки, хранения, комбинирования, передачи и любого другого использования персональных данных в ГБУЗ АО «ОКПБ».

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами, действующими на территории Российской Федерации.

1.3. Все изменения в Положение вносятся приказом по ГБУЗ АО «ОКПБ».

1.4. Все работники ГБУЗ АО «ОКПБ», участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

2. Термины и определения

2.1. В настоящем Положении используются следующие основные термины и определения:

- персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его

фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных субъекта ПДн;
- оператор персональных данных (далее по тексту оператор ПДн) - лицо, организующее или осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки ПДн;
- субъект персональных данных (далее по тексту субъект ПДн) - физическое лицо, вступившее в трудовые отношения с оператором персональных данных, а также пользующееся медицинскими или иными услугами, предоставляемыми ГБУЗ АО «ОКПБ»;
- конфиденциальность персональных данных - обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным субъектов ПДн, требование не допускать их распространения без согласия субъекта ПДн или иного законного основания;
- распространение персональных данных - действия, направленные на передачу персональных данных субъектов ПДн определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных субъектов ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным субъектов ПДн каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом (оператором ПДн) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов ПДн либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных субъектов ПДн, в том числе их передачи;
- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных субъектов ПДн;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту ПДн;
- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- информация - сведения (сообщения, данные) независимо от формы их представления;
- работники - лица, имеющие трудовые отношения с ГБУЗ АО «ОКПБ», либо кандидаты на вакантную должность, вступившие в отношения с ГБУЗ АО «ОКПБ» по поводу приема их на работу.
- пациенты – лица, обратившиеся в ГБУЗ АО ОКПБ за оказанием медицинской помощи.

3. Состав персональных данных

3.1. В состав персональных данных входят:

3.1.1. Персональные данные работников - сведения, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, а также о предыдущих местах их работы.

3.1.2. Персональные данные пациентов - сведения, содержащие информацию о паспортных данных, месте жительства, состоянии здоровья.

3.2. К персональным данным относятся:

- сведения, содержащиеся в документах, удостоверяющих личность;
- информация, содержащаяся в трудовой книжке;
- информация, содержащаяся в документах воинского учета;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования (снилс);
- информация об образовании, квалификации или наличии специальных знаний или подготовки;
- информация о состоянии здоровья в случаях, предусмотренных законодательством;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории российской федерации (инн);

- сведения о семейном положении;
- информация о заработной плате;
- другая персональная информация, позволяющая идентифицировать субъекта персональных данных;

3.3. К документам, содержащим информацию персонального характера, относятся:

- документы, удостоверяющие личность или содержащие информацию персонального характера;
- учетные документы по личному составу, а также вспомогательные регистрационно-учетные формы, содержащие сведения персонального характера;
- трудовые договоры с работниками, изменения к трудовым договорам, договоры о материальной ответственности с работниками;
- распорядительные документы по личному составу;
- документы по оценке деловых и профессиональных качеств работников при приеме на работу;
- документы, отражающие деятельность конструктивных и аттестационных комиссий;
- документы о результатах служебных расследований;
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству учреждения, руководителям структурных подразделений и служб;
- копии отчетов, направленных в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие организации и учреждения;
- документы бухгалтерского учета, содержащие информацию о расчетах персоналом;
- медицинские документы, справки;
- другие документы, содержащие сведения персонального характера.

4. Получение персональных данных

4.1. Персональные данные субъекта ПДн предоставляются самим субъектом ПДн. Если персональные данные субъекта ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено

письменное согласие. Оператор ПДн должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных и последствиях отказа субъекта ПДн дать согласие на их получение.

4.2. Субъект ПДн обязан предоставлять оператору ПДн достоверную персональную информацию. При изменении персональных данных субъект персональных данных обязан письменно уведомить об этом оператора в срок, не превышающий 14 дней. Оператор ПДн имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

4.3. Оператор ПДн не имеет права получать и обрабатывать персональные данные о его политических, религиозных и иных побуждениях, в соответствии со ст. 24 Конституции Российской Федерации.

4.4. Данные о частной жизни субъекта ПДн оператор ПДн вправе получать и обрабатывать только с его письменного согласия.

4.5. Оператор ПДн не имеет права получать и обрабатывать персональные данные субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных ТК РФ или иными федеральными законами.

4.6. При принятии решений, затрагивающих интересы работника, оператор ПДн не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5. Обработка персональных данных

5.1. Обработка персональных данных осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъектов, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а также оказании медицинских услуг пациентам, сбор, анализ и обработка статистической информации.

5.2. При обработке персональных данных в информационной системе персональных данных должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- **постоянный контроль над обеспечением уровня защищенности персональных данных.**

5.3. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

5.4. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники оператора ПДн или лица, осуществляющие такую обработку по договору с оператором ПДн), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором ПДн без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

5.5. Требования к передаче персональных данных работников ГБУЗ АО «ОКПБ»:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью

работника, а также в других случаях, предусмотренных законодательством РФ;

- не сообщать персональные данные работника в коммерческих целях без письменного согласия;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, определенным приказом по учреждению, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом трудовой функции;
- передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

5.6. Персональные данные пациента подлежат передаче исключительно в соответствии с законодательством РФ (Федеральный закон № 323-ФЗ от 21 ноября 2011 г. «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон № 3185-1 от 2 июля 1992 года «О психиатрической помощи и гарантиях прав граждан при её оказании», Федеральный закон № 326-ФЗ от 29 ноября 2010 г. «Об обязательном медицинском страховании в Российской Федерации» и др.).

5.7. Без согласия пациента или его законного представителя допускается предоставление сведений согласно части 4 статья 13 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации»:

- в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением уголовно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

- в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 ФЗ «Об основах охраны здоровья граждан в Российской Федерации», для информирования одного из его родителей или иного законного представителя;
- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;
- в целях расследования несчастного случая на производстве и профессионального заболевания;
- при обмене информацией медицинскими организациями, в том числе разрешенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;
- в целях осуществления учета и контроля в системе обязательного социального страхования;
- в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

5.8. Подразделения, а также работники ГБУЗ АО «ОКПБ», в обязанности которых входит работа с персональными данными, обеспечивают защиту персональных данных от несанкционированного доступа и копирования.

5.9. Автоматизированное хранение и обработка персональных данных осуществляется с использованием специализированного программного обеспечения, отвечающего требованиям информационной безопасности.

6. Доступ к персональным данным

6.1. Внутренний доступ (работники ГБУЗ АО «ОКПБ»).

6.1.1. Доступ к персональным данным разрешен только уполномоченным должностным лицам, которые непосредственно используют их в служебных целях, и/или назначенные приказом главного врача. Перечень лиц имеющих доступ к персональным данным указывается в «Положении о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных».

6.1.2. Уполномоченные лица имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций в

соответствии с должностной инструкцией указанных лиц. Все остальные работники имеют право на полную информацию только об их персональных данных и обработке этих данных.

6.2. Внешний доступ к персональным данным имеют работники контрольно - ревизионных органов при наличии документов, являющихся обоснованием к работе с персональными данными, а так же иные лица в соответствии с действующим законодательством.

7. Организация защиты персональных данных

7.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается и организуется комиссией по информационной безопасности ГБУЗ АО «ОКПБ».

7.2. Общую организацию защиты персональных данных осуществляет начальник службы безопасности совместно с начальником отделения автоматизированных систем управления.

7.3. Начальник службы безопасности организует:

- ознакомление под роспись работников, которые участвуют в обработке персональных данных, с настоящим Положением;
- истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных субъекта и соблюдении правил их обработки;
- общий контроль соблюдения работниками ГБУЗ АО «ОКПБ» мер по защите персональных данных субъекта.

7.4. Организацию и контроль защиты персональных данных физических лиц в структурных подразделениях ГБУЗ АО «ОКПБ», работники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

7.5. Защите подлежат:

- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.

7.6. Защита сведений, хранящихся в электронных базах данных ГБУЗ АО «ОКПБ», от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается Системой защиты персональных данных.

8. Хранение персональных данных

8.1. Персональные данные пациентов хранятся в электронном виде в локальной компьютерной сети. Защита доступа к электронным базам данных, содержащим персональные данные пациента, обеспечивается Системой защиты персональных данных.

8.2. Работник ГБУЗ АО «ОКПБ», имеющий доступ к персональным данным пациентов в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные пациента, исключающее доступ к ним третьих лиц;
- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия на своем рабочем месте, сотрудник обязан передать документы и иные носители, содержащие персональные данные пациентов лицу, на которое локальным актом ГБУЗ АО «ОКПБ» (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

8.3. При увольнении сотрудника, имеющего доступ к персональным данным пациентов, документы и иные носители, содержащие персональные данные субъектов, передаются другому работнику, имеющему доступ к персональным данным пациентов по указанию руководителя структурного подразделения.

8.4. Помещения, в которых хранятся персональные данные пациентов, оборудуются надежными замками, сейфами, а в установленных случаях системой сигнализации.

9. Уничтожение персональных данных

9.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке и в сроки, предусмотренные архивным законодательством Российской Федерации.

9.2. Персональные данные подлежат уничтожению по достижению целей обработки, или в случае утраты необходимости в достижении таких целей.

9.3. Режим конфиденциальности персональных данных снимается в случае их обезличивания.

10. Права субъекта персональных данных

по обеспечению защиты своих персональных данных

10.1. Субъекты ПДн имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;

- доступ к своим медицинским данным с помощью медицинского специалиста по своему выбору;
- обжалование в суд любых неправомерных действий или бездействия при обработке и защите его персональных данных.

11. Ответственность за разглашение информации, связанной с персональными данными

11.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

11.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

11.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.4. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

11.5.1. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

11.5.2. Должностные лица, в обязанность которых входит ведение персональных данных субъектов, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

**Приложение № 1
к «Положению о защите персональных данных»,
утвержденному приказом главного врача
№ 151 от 16.08.2013 года**

Согласие работника на обработку его персональных данных

Я, _____,

(Ф.И.О. полностью)

являясь работником государственного бюджетного учреждения здравоохранения Астраханской области «Областной клинической психиатрической больницы» (далее - Оператор), расположенной по адресу г. Астрахань, ул. Началовское шоссе 15, подтверждаю своё согласие на обработку моих персональных данных Оператором включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу, обезличивание, блокирование, уничтожение:

1. Для формирования общедоступных источников персональных данных (справочников, размещения информации в СМИ и на сайте Учреждения) в следующем составе: фамилию, имя, отчество; сведения о профессии, должности, образовании, квалификации, номер рабочего телефона, иные персональные сведения, предоставленные мной Оператору для размещения в общедоступных источниках.
2. Для передачи моих персональных данных органам местного самоуправления, государственным органам и организациям, страховым организациям, контрольно-надзорным органам для целей обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности, аттестации, контроля качества выполняемой работы и обеспечения сохранности имущества, оформления доверенностей, конкурсного отбора, поощрения (награждения), прохождения безналичных платежей на мой банковский счет. Для этих целей могут быть получены или переданы сведения о дате рождения, гражданстве, паспортных данных, месте жительства, предыдущих местах работы, состоянии в браке, составе семьи, сведения о воинском учете, идентификационном номере налогоплательщика, [свидетельстве](#) государственного пенсионного страхования, допуске к сведениям, составляющим государственную тайну, доходах, социальных льготах и выплатах, на которые я имею право в соответствии с действующим законодательством, о состоянии здоровья в части вопросов, о возможности выполнения работником трудовой функции.

Вышеприведенное согласие на обработку моих персональных данных представлено с учетом п. 2 ст. 6 и п. 2 ст. 9 Федерального закона «О персональных данных» №152-ФЗ от 27.07.2006 года, в соответствии с которыми обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения договора, стороной в котором я являюсь, может осуществляться Оператором без моего дополнительного согласия.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора с Оператором и может быть отозвано путем подачи Оператору письменного заявления с указанием причин отзыва.

" ____ " _____ 20__ г.

_____ / _____

(подпись)

(расшифровка Ф.И.О.)