Положение о защите персональных данных пациентов в Государственном автономном учреждении здравоохранения Амурской области «Амурская областная клиническая больница»

СОДЕРЖАНИЕ

ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин /сокращение	Значение
АРМ	Автоматизированное рабочее место пользователя
ИС	Информационная система
ИСПДн	Информационная система персональных данных
МО	Медицинская организация
ПДн	Персональные данные
СУБД	Система управления базами данных
РИСЗ Амурской области	Региональная информационная система в сфере здравоохранения Амурской области
Оператор	Государственное автономное учреждение здравоохранения Амурской области «Амурская областная клиническая больница»
ЦОД	Центр обработки данных ГБУЗ АО «Амурский медицинский информационно-аналитический центр»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение об обработке и защите персональных данных в РИСЗ Амурской области Государственного автономного учреждения здравоохранения Амурской области «Амурская областная клиническая больница» (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных, в соответствии с законодательством Российской Федерации и гарантии конфиденциальности персональных данных.

Настоящее Положение определяет также, правила накопления, хранения, защиты и уничтожения при не автоматизированной обработке персональных данных.

Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.06г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.06г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.04г. №98-ФЗ «О коммерческой тайне», Федеральным законом от 22.10.04г. № 125-ФЗ «Об архивном деле в Российской Федерации», указанием Федерального агентства по образованию от 22. 10. 09г. №17-187 «Об обеспечении защиты персональных данных», Федеральным законом РФ от 22.07.1993г. № 5487-1 «Основы законодательства Российской Федерации об охране здоровья граждан», Постановление Правительства РФ от 15 сентября 2008г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.10.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. ОСНОВНЫЕ ПОНЯТИЯ

Для целей настоящего Положения используются следующие понятия:

Оператор персональных данных (далее оператор) - Государственное автономное учреждение здравоохранения Амурской области «Амурская областная клиническая больница», осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных;

Персональные данные - 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, информация о состоянии здоровья, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

Субъект – субъект персональных данных.

Персональные данные пациента - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

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.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

3. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

При обработке персональных данных должны соблюдаться следующие требования:

- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

3.1. Оператор при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

- обработка персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, для осуществления государственной политики в сфере здравоохранения, обеспечивающей необходимые условия при реализации прав гражданина на охрану здоровья, получение медицинской помощи, лекарственного обеспечения, участия в реализации государственной политики в области обязательного медицинского страхования граждан в соответствии с законодательством Российской Федерации и Амурской области, контроля количества и качества оказанной пациенту медицинской помощи;
- при определении объема и содержания, обрабатываемых персональных данных пациента, Оператор должен руководствоваться Конституцией Российской Федерации, Федеральным законом № 323-ФЗ «Об основах

охраны здоровья граждан в Российской Федерации», законодательством РФ в сфере защиты персональных данных и обработки информации, и иными Федеральными законами и региональными нормативными актами в области защиты персональных данных.

- защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном Федеральным законом и другими нормативными документами;
- пациенты или их представители по их запросу должны быть ознакомлены с документами Оператора, устанавливающими порядок обработки персональных данных пациентов, а также об их правах и обязанностях в этой области.

4. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные поступают в РИСЗ Амурской области из двух источников – импорт данных регионального фрагмента реестра застрахованных ОМС и непосредственный сбор непосредственно от субъекта персональных данных.

При сборе персональных данных должны соблюдаться следующие требования:

- Субъект самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку оператором.
- В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных и дает письменное согласие на их обработку оператором.
- Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.
- Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных, в случае импорта персональных данных из регионального фрагмента реестра застрахованных ОМС, других случаях, предусмотренных Федеральным и Региональным законодательством.
- Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.
- Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

5. ХРАНЕНИЕ И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При хранении и обработке персональных данных в РИЗС АО должны соблюдаться следующие требования:

- Персональные данные пациентов хранятся в электронном виде на сервере баз данных РИСЗ Амурской области. Доступ к электронным базам данных ограничен логином и паролем.
- Возможна передача персональных данных пациентов по внутренней сети Оператора с использованием технических и программных средств защиты информации, с доступом только для работников Оператора, допущенных к работе с персональными данными работников, приказом главного врача и только в объеме, необходимом данным работникам для выполнения своих должностных обязанностей.
- Для обеспечения хранения персональных данных пациентов определяются следующие оснащенные средствами защиты рабочих мест: Помещение регистратуры Оператора, врачебные кабинеты, ординаторские стационарных отделений и другие помещения, где находятся АРМ, имеет ограниченный доступ в течение рабочего дня, по окончании рабочего дня помещение закрывается на ключ.
- Здания Оператора находятся под круглосуточной охраной и имеют систему видеонаблюдения. Также здания снабжены пожарной сигнализацией.
- Хранение персональных данных пациентов осуществляется не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению, в течение тридцати дней, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не установлено действующим законодательством.

5.2. При хранении и неавтоматизированной обработке персональных данных соблюдаются следующие требования:

- По окончании рабочего дня помещение регистратуры закрывается на ключ и опечатывается. Ключ сдается на пост охраны.

- Сдача медицинских карт персоналом Оператора, после приема больных осуществляется в течение рабочего дня, либо по его окончании. Персонал Оператора несет личную ответственность в случае не передачи карт на хранение в регистратуру Оператора.
- В стационарах медицинские карты пациентов хранятся в ординаторских, в запираемых шкафах.
- Персональные данные подлежат уничтожению, в течение тридцати дней, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не установлено действующим законодательством.
- При неавтоматизированной обработке персональных данных на бумажных носителях:

  - не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
  - персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

5.3. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах) исключающих доступ посторонних лиц. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность. Доступ в служебные помещения имеют сотрудники допущение к обработке персональных данных, согласно утвержденного главным врачом списка. Уборка таких служебных помещений проводится в рабочее время в присутствии сотрудников допущенных к обработке персональных данных.

5.4. 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, вымарывание).

5.5. Уничтожение бумажных носителей должно осуществляться сотрудниками, допущенными к обработке персональных данных, путем, не

допускающим дальнейшую возможность ознакомления с данными документами (измельчение, сжигание).

5.6. Решение об уничтожении принимается Главным врачом на основании ходатайства ответственного за соблюдение режима конфиденциальности, либо ответственного за уничтожение медицинских карт пациентов.

5.7. Уничтожение электронных и бумажных носителей проводится комиссией с составлением акта списания электронных, бумажных носителей информации (приложение №1). Уничтожение материальных носителей проводится путем измельчения материального носителя, либо его сжигания и составлением акта списания, за подписью ответственных лиц.

5.8. Лица допущенные к сбору, обработке, хранению, уничтожению и т.д. персональных данных, дают обязательство о неразглашении, по форме в приложении №2

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

При передаче персональных данных должны соблюдаться следующие требования:

- Передача персональных данных пациентов третьим лицам осуществляется Оператором только с письменного согласия пациента, с подтверждающей визой главного врача, за исключением случаев, предусмотренных статьей 13 ФЗ № 323:

  ✓ в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учётом положений пункта 1 части 9 статьи 20 указанного Федерального закона;

  ✓ при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

  ✓ по запросу органов дознания и следствия, 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 условно 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 указанного Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 указанного Федерального закона, 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 причинён в результате противоправных действий;

  ✓ в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) 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 размещенной 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 указанным Федеральным законом.

- Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками несут ответственность за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
- Оператор обеспечивает ведение журнала учета выданных персональных данных пациентов, 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 законом на получение персональных данных пациента, либо отсутствует письменное согласие пациента на предоставление его персональных данных, Оператор обязан отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдаётся в мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится у Оператора.
- В целях выполнения необходимых условий для реализации конституционных прав граждан на охрану здоровья, получение медицинской

помощи, лекарственного обеспечения, профилактики инвалидности и медицинской реабилитации инвалидов, оказания медицинской и профилактической помощи населению, санаторно-курортного лечения возможна передача персональных данных пациентов при наличии письменного согласия пациента, в уполномоченные региональные и федеральные органы исполнительной власти по отрасли здравоохранения и социального развития, федеральные и региональные Фонды, страховые медицинские организации, другие медицинские и фармацевтические организации, участвующие в реализации Программы государственных гарантий оказания гражданам бесплатной медицинской помощи, в том числе государственной политики в области обязательного медицинского страхования граждан и ДМС, реализации приоритетных национальных проектов и целевых программ по отрасли здравоохранение, обеспечении отдельных категорий граждан необходимыми лекарственными средствами, а также работодателю – в случаях проведения профилактических медицинских осмотров в соответствии с заключенным между Оператором и работодателем пациента договором.

- Передача указанных сведений и документов осуществляется с согласия пациента. Согласие пациента оформляется письменно в виде отдельного документа. После получения согласия пациента дальнейшая передача указанных сведений и документов, данных лицам дополнительного письменного согласия не требует.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

Защита информации, в том числе персональных данных, представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа,
- реализацию права на доступ к информации.

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

- АРМ, с которых осуществляется доступ к персональным данным (БД РИСЗ Амурской области), защищены паролями доступа. Пароли устанавливаются Администратором безопасности Учреждения или системны администратором и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов на данном АРМ.
- Иные меры, предусмотренные Положением об организации работ по обеспечению проведению безопасности ПДн при их обработке в ИСПДн.
- Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 01.11. 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8. ПРАВА И ОБЯЗАННОСТИ ПАЦИЕНТА В ОБЛАСТИ ЗАЩИТЫ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях обеспечения защиты персональных данных, хранящихся у Оператора, пациенты имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, за исключением случаев, предусмотренных федеральным законом; Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Оператор обязан сообщить пациенту или его законному представителю информацию о наличии персональных данных, относящихся к пациенту, а также предоставить возможность ознакомления с ними пациента или его законного представителя при обращении либо в течение десяти рабочих дней с даты получения запроса пациента или его законного представителя. В случае отказа в предоставлении пациенту или его законному представителю информации о наличии персональных данных Оператор обязан дать в письменной форме мотивированный ответ в срок, не превышающий семи рабочих дней со дня обращения/ получения запроса пациента или его законного представителя;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Положения;
- обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите персональных данных.
- иные права, предусмотренные действующим законодательством.

9. ПРОЧИЕ ПОЛОЖЕНИЯ

Настоящее Положение вступает в силу с даты его утверждения.

При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании приказа Главного врача.

Настоящее Положение распространяется на всех пациентов, обработка чьих персональных данных осуществляется с использованием РИСЗ Амурской области, а так же сотрудников Оператора имеющих доступ и осуществляющих перечень действий с персональными данными пациентов.

Данное положение так же распространяется на не автоматизированную обработку персональных данных.

10. ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ

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

Приложение № 1
к приказу Государственного автономного
учреждения здравоохранения Амурской области
«Амурская областная клиническая больница»
от «___» _____ 20 ___ г.

У Т В Е Р Ж Д А Ю

Главный врач ГАУЗ АО АОКБ

_____

«_____» ___ _____2016 г.

Приложение №1

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от №___ в составе:
_____
_____
(должности, ФИО)

провела отбор носителей конфиденциальной информации (персональных данных), не подлежащих дальнейшему хранению:

№ п/п	**Дата**	**Учетный номер носителя**	**Примечание**

Всего носителей _____(цифрами и прописью)

На носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные носители уничтожены
_____
путем (разрезания, демонтажа и т.п.) ,
_____

Председатель комиссии Подпись Дата
Члены комиссии
(ФИО) Подпись Дата

Приложение №2
к приказу Государственного автономного
учреждения здравоохранения Амурской области
«Амурская областная клиническая больница»
№ 06-169/1 от «01» марта 20 16 г.

Обязательство
о неразглашении конфиденциальной информации
(персональных данных)

Я_____,
(ФИО)

Исполняющий(ая) должностные обязанности по замещаемой должности
_____
(должность, наименование структурного подразделения)

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с трудовыми обязанностями, должностным регламентом (должностной инструкцией), мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащей сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей (врачебной тайной).
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей (врачебной тайной).
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику, а также лицу, ответственному за организацию защиты информации в Государственном автономном учреждении здравоохранения Амурской области «Амурская областная клиническая больница».
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. После прекращения трудового договора и увольнения из Государственного автономного учреждении здравоохранения Амурской области «Амурская областная клиническая больница», прекратить обработку известных мне 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) (подпись)

« ___ »_____20___ г.