Приложение № 1 к приказу ОГБУЗ ИОКТБ
от «15» июня 2017 № 158

ПОЛОЖЕНИЕ

Об обработке и защите персональных данных
в Областном государственном бюджетном учреждении здравоохранения «Иркутская областная клиническая туберкулезная больница»

1. Термины и определения

- Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;
- Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;
- Оператор персональных данных – 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;
- Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- Обработка персональных данных – 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;
- Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
- 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;
- 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;
- Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- Субъект персональных данных (субъект) – (в рамках настоящего Положения) физическое лицо, чьи персональные данные обрабатываются в Областном

государственном бюджетном учреждении здравоохранения «Иркутская областная клиническая туберкулезная больница» (далее – Учреждение, Оператор) в процессе осуществления своей деятельности. К таким субъектам относятся сотрудники Учреждения; пациенты, обратившиеся в Учреждение за медицинской помощью.

2. Общие положения

2.1. Настоящее Положение закрепляет права субъектов и обязанности Оператора в области персональных данных, а также устанавливает требования к обеспечению безопасности персональных данных при их обработке с использованием средств автоматизации и без использования таких средств.

2.2. Настоящее Положение разработано в соответствии с требованиями следующих нормативных правовых документов:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15 сентября 2008 г. N 687);
- Федеральный закон от 22 октября 2004 г. N 125-ФЗ «Об архивном деле в Российской Федерации».

2.3. Все должностные лица, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись. Перечень лиц, допущенных к обработке персональных данных, устанавливается приказом главного врача Учреждения

2.4. Лицо, ответственное за организацию обработки персональных данных, назначается приказом главного врача Учреждения.

2.5. Лицо, ответственное за безопасность информационных систем персональных данных (администратор безопасности ИСПДн) назначается приказом главного врача Учреждения.

2.6. Положение вступает в силу с момента его утверждения главным врачом Учреждения.

2.7. Все изменения в настоящее Положение утверждаются приказом главного врача Учреждения с обязательным доведением изменений до ответственных сотрудников. Настоящее Положение может дополняться другими документами (инструкциями, положениями, регламентами), не противоречащими настоящему Положению, утверждаемыми в установленном порядке главным врачом Учреждения.

3. Обработка персональных данных

3.1. Обработка персональных данных в Учреждении ведется в целях:

- реализации функций работодателя (ведение личного дела работника, уплата налогов и отчислений в пенсионный фонд, начисление зарплаты и др.) и обеспечения трудовой деятельности;
- оказания медицинских услуг в соответствии с Уставом.

3.2. Обработка персональных данных в Учреждении должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных;
- 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.

3.3. Учреждение осуществляет обработку персональных данных субъектов персональных данных в соответствующих информационных системах персональных данных (ИСПДн), либо в бумажной форме. В Учреждении составляются «Перечень персональных данных» и «Перечень информационных систем персональных данных», которые утверждаются главным врачом Учреждения.

3.4. При обработке персональных данных Учреждение обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3.5. Должностные лица Учреждения, допущенные к обработке персональных данных, подписывают Обязательство о неразглашении персональных данных по форме, представленной в Приложении 1 к настоящему Положению.

3.6. Лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

3.7. В случае, если Учреждение на основании договора поручает обработку персональных данных или передает данные другому лицу (организации), одним из существенных условий договора должна являться обязанность обеспечения указанным лицом (организацией) конфиденциальности персональных данных и безопасности персональных данных при их обработке.

3.8. Учреждение осуществляет следующие виды обработки персональных данных: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.9. Учреждение не осуществляет следующие виды обработки персональных данных:

- трансграничной передачи персональных данных;
- обработки персональных данных в целях продвижения товаров, работ, услуг на рынке и политической агитации;
- принятие решений на основании исключительно автоматизированной обработки персональных данных в информационных системах (то есть автоматической обработки – без участия человека).

3.10. Обработка персональных данных может быть прекращена по следующим причинам:

- достижение цели обработки персональных данных;

- прекращение действия договора/поручения обработки персональных данных;
- запрос субъекта ПДн о прекращении обработки его персональных данных;
- прекращение деятельности Учреждения.

4. Порядок обработки персональных данных в ИСПДн с использованием средств автоматизации

4.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119. Также, в соответствии с данным постановлением, оператором проводится установление уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от типа ИСПДн, актуальных угроз и количества обрабатываемых данных субъектов. Установление уровней защищенности ПДн подтверждается соответствующими актами, составленными и подписанными постоянной комиссией по персональным данным. Состав такой комиссии утверждается приказом главного врача Учреждения.

4.2. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.3. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-распорядительных документов о порядке эксплуатации информационных систем персональных данных, включающих в себя акт установления уровней защищенности ПДн, инструкции допущенного к обработке пользователя, администратора безопасности ИСПДн, по организации антивирусной/парольной защиты, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

5. Порядок обработки персональных данных в ИСПДн без использования средств автоматизации

5.1. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях, на внешних электронных носителях) осуществляется в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации 15.09.2008г. №687.

5.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.3. 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);
- документы, содержащие персональные данные, могут формироваться в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, — при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.5. Неавтоматизированная обработка персональных данных в электронном виде заключается в хранении, передаче, уничтожении внешних электронных носителей информации.

5.6. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета машинных носителей персональных данных, составленном по утвержденной форме.

5.7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не

подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- 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.

5.8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях и/или в надежно запираемых металлических шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.9. 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).

6. Порядок получения (сбора, уточнения и накопления) персональных данных

6.1. Все обрабатываемые персональные данные могут быть получены непосредственно от субъектов персональных данных или их законных представителей после подписания Согласия на обработку персональных данных (Приложение 3), если иное не указано в договорах с соответствующими операторами.

6.2. Сбор, уточнение и накопление персональных данных в информационных системах Учреждения может осуществляться допущенными к обработке ПДн сотрудниками Учреждения.

6.3. Уточнение любых неполных, неточных или устаревших данных производится Учреждением в порядке, установленном ст. 20-21 Федерального закона №152 «О персональных данных», при получении полных, точных или актуальных данных соответственно. О внесенных таким образом изменениях Учреждение уведомляет соответствующего субъекта персональных данных, а также по возможности лиц, которым в установленном порядке были предоставлены соответствующие персональные данные.

7. Порядок привлечения специализированных сторонних организаций к разработке ИСПДн и систем защиты информации

7.1. Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых ИСПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн определяются ответственным за организацию обработки ПДн, исходя из особенностей автоматизированных систем и по согласованию с администратором безопасности ИСПДн.

7.2. Контроль за эксплуатацией ИСПДн осуществляется администратором безопасности ИСПДн.

7.3. К проектированию систем защиты персональных данных в ИСПДн, а также проведению мероприятий по обеспечению безопасности персональных данных для ИСПДн (поставка и внедрение средств защиты информации) могут привлекаться сторонние специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

8. Порядок предоставления персональных данных

8.1. Персональные данные предоставляются в виде сводных отчетов/перечней/ реестров третьим сторонам на основании соответствующих соглашений или договоров. При этом одним из ключевых условий договора/соглашения должно быть соблюдение конфиденциальности третьей стороной получаемых персональных данных.
8.2. Персональные данные могут предоставляться третьим лицам также в следующих случаях:

- если было получено (и не отозвано) согласие субъекта на предоставление его персональных данных третьим лицам;
- по запросу правоохранительных, судебных, исполнительных органов и других учреждений, которые имеют на это право, в предусмотренных действующим законодательством случаях.

8.3. Предоставление субъекту (или его законному представителю) персональных данных субъекта производится при обращении субъекта или поступлении запроса субъекта (или его законного представителя) в порядке, установленном Федеральным законом №152-ФЗ «О персональных данных».
8.4. Предоставление персональных данных третьим лицам может осуществляться путем передачи на материальных носителях (бумажных или машинных). Перед предоставлением персональные данные извлекаются из информационной системы на данный носитель (путем извлечения, печати, копирования и т.п.).
8.5. Персональные данные, передаваемые по каналам в электронном виде (Интернет, электронная почта и др.), могут передаваться только по защищенным каналам связи с использованием сертифицированных ФСБ России шифровальных (криптографических) средств.
8.6. Передача персональных данных по открытым каналам связи (в т.ч. по телефону/факсу или телеграфу) запрещается.

9. Порядок хранения, блокирования и уничтожения персональных данных

9.1. Персональные данные могут храниться до достижения целей обработки или до востребования (передачи всех носителей субъекту или третьему лицу).
9.2. Персональные данные, предоставленные Учреждению оператором по договору, при окончании срока указанного договора уничтожаются.
9.3. Блокирование или уничтожение неполных, устаревших, неточных персональных данных осуществляется ответственным работником при получении соответствующего требования субъекта персональных данных или его законного представителя.
9.4. По достижении целей обработки персональные данные блокируются и хранятся в течение срока временного хранения, установленного в соответствии с архивным законодательством Российской Федерации.
9.5. По истечении срока временного хранения персональные данные уничтожаются или предоставляются на постоянное хранение в Государственный архив.
9.6. Виды бумажных и машинных носителей персональных данных, методы защиты от несанкционированного доступа, порядок хранения и уничтожения персональных данных устанавливаются локальными нормативными актами Учреждения, в частности – Положением о порядке хранения и уничтожения ПДн.

10. Доступ лиц к персональным данным

10.1. Перечень лиц, допущенных к обработке персональных данных, а также права доступа указанных лиц, устанавливаются локальными нормативными актами.

10.2. Должностные лица, которым необходимо получить доступ к обработке персональных данных для выполнения своих непосредственных должностных обязанностей, должны быть ознакомлены с настоящим Положением под роспись, а также подтвердить свои обязанности по обеспечению безопасности персональных данных, подписав Обязательство о неразглашении персональных данных.

10.3. Исключительное право доступа к любым персональным данным, обрабатываемым в Учреждении, имеют следующие должностные лица: главный врач, администратор безопасности ИСПДн и ответственный за организацию обработки персональных данных.

10.4. В отличие от предоставления персональных данных доступ к персональным данным не подразумевает извлечения персональных данных за пределы информационных систем персональных данных.

11. Права субъектов и обязанности Оператора в области обработки персональных данных

11.1. Субъект персональных данных имеет право по запросу, в установленных законом случаях:

- узнать, ведется ли в Учреждении обработка его персональных данных (в соответствии с п.7, ст. 14, 152-ФЗ);
- получить у Оператора свои персональные данные, обрабатываемые в Учреждении, за исключением случаев, когда это нарушает права и законные интересы третьих лиц (а также других случаев, установленных законом);
- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, или неточными;
- узнать юридические последствия обработки (или отказа от обработки) персональных данных в Учреждении;
- обжаловать действия или бездействия Оператора, в случае если субъект считает их нарушающими его права и свободы, в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

11.2. Учреждение, как Оператор ПДн, обязана:

- принимать необходимые правовые, организационные и технические меры по защите персональных данных от неправомерных и случайных действий или утраты (в соответствии со ст.ст. 18-22, 152-ФЗ);
- предоставить субъекту или его законному представителю, оператором персональных данных которого является Учреждение, все обрабатываемые сведения о нем, безвозмездно, в доступной форме и без персональных данных других субъектов;
- осуществить уточнение, блокирование или уничтожение персональных данных субъекта при предоставлении субъектом (или его законным представителем) сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту, являются неполными, устаревшими или неточными.

12. Ответственность за нарушение требований настоящего Положения

12.1. При получении (сборе, уточнении, накоплении) персональных данных непосредственно от субъектов или их законных представителей, они несут ответственность за актуальность и точность предоставленной ими информации.

12.2. Должностные лица, осуществляющие ввод, накопление, уточнение и другие виды обработки ПДн в информационных системах, несут ответственность за полноту полученной информации и не должны вводить информацию, противоречащую полученной непосредственно от субъектов персональных данных или их законных представителей.

12.3. Лица, виновные в нарушении норм, регулирующих обработку персональных данных субъектов, несут материальную, дисциплинарную, административную, гражданско-правовую и уголовную ответственность в порядке, установленном действующим законодательством Российской Федерации.

12.4. Учреждение несет установленную законом ответственность перед субъектами персональных данных за неправомерные действия ответственных лиц с персональными данными указанных субъектов. Уполномоченные лица несут ответственность перед оператором по договору.