УТВЕРЖДЕНО
Главный врач ГБУЗ «СОНД»
С.А.Корякин

от _*09.01.2014*_ № __*87*___

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в Государственном бюджетном учреждении здравоохранения «Самарский областной наркологический диспансер».

1. Общие положения

1.1. Настоящее Положение о порядке обработки персональных данных в ГБУЗ «Самарский областной наркологический диспансер» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 21.12.2013 г.) «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствий с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; постановлением Правительства Российской Федерации от 20 июля 2013 г. N 607 "О внесении изменений в перечень 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", постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств

автоматизации», правовых актов уполномоченных федеральных органов исполнительной власти и устанавливает единый порядок обработки персональных данных в ГБУЗ «Самарский областной наркологический диспансер» (далее – Диспансер). Настоящее положение определяет основные направления деятельности Диспансера в области обработки конфиденциальной информации. По мере развития материально-технической базы Диспансера, кадрового состава и действующего законодательства настоящее положение и приложения к нему будут корректироваться.

1.2. В целях настоящего Положения используются следующие термины и понятия:

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, семейное, имущественное положение, образование, профессия, доходы, сведения о состоянии здоровья, медицинский диагноз, другая информация;

конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, являющихся государственной тайной, а составляющая служебную или коммерческую ценность в силу неизвестности ее третьим лицам, и к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

специальные категории персональных данных - данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов 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;

информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

обработка персональных данных без использования средств автоматизации (не автоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

разглашение (несанкционированное распространение) служебных сведений - ознакомление с ними лиц, не являющихся работниками Диспансера и не имеющих к этим сведениям непосредственного отношения, лицом, которому эти сведения были доверены или стали известны по службе или по работе, без указания или разрешения соответствующего должностного лица.

Технологический процесс обработки конфиденциальной информации Диспансера предусматривает два способа обработки — обработка с использованием и без использования средств автоматизации.

2. Условия проведения обработки персональных данных

2.1. Обработка персональных данных осуществляется:

после получения письменного согласия субъекта персональных данных, составленного по форме согласно приложению 1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Самарской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;

после принятия необходимых организационных и технических мероприятий по защите персональных данных, в соответствии с действующим законодательством.

3. Организационные меры по защите персональных данных

3.1 В Диспансере распоряжением главного врача назначается сотрудник, ответственный за обеспечение безопасности персональных данных.

3.2 В Диспансере утверждают актом главного врача следующие документы:

- правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в

соответствии с ним нормативными правовыми актами и локальными актами оператора;

- правила работы с обезличенными данными;

- перечень информационных систем персональных данных;

- перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

- перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

- перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

- должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного или муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

- типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

- порядок доступа сотрудников Диспансера в помещения, в которых ведется обработка персональных данных;

3.3 Лица, допущенные к обработке персональных данных, как с помощью информационных систем персональных данных, так и без использования средств автоматизации, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают типовое обязательство служащего о неразглашении

информации, содержащей персональные данные, по форме согласно утвержденной главным врачом.

3.4 При обработке персональных данных в Диспансере запрещается:

обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке и осуществлять ввод персональных данных под диктовку.

3.5 В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Диспансера докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии

4. Технические меры по защите персональных данных

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации в соответствии с приказами ФСТЗК от 11 февраля 2013 № 17 и от 18 февраля 2013 г № 21. В зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности информации;

- целостность информационной системы и информации;

- доступность информации;

- защиту среды виртуализации;

- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных;

- установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

- централизованное управление системой защиты информации информационной системы, инвентаризация и контроль за лицензионной чистотой программного обеспечения.

5. Условия обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

5.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствий с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; постановления Правительства Российской Федерации от 20 июля 2013 г. N 607 "О внесении изменений в перечень 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", нормативных правовых актов уполномоченных федеральных органов исполнительной власти.

5.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

при отсутствии установленных и настроенных сертифицированных средств защиты информации;

при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

6. Условия обработки персональных данных без использования средств автоматизации

6.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.2. При не автоматизированной обработке различных категорий персональных данных должен использоваться отдельный носитель для каждой категории персональных данных.

6.3. При не автоматизированной обработке персональных данных на материальных носителях:

не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются 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.

6.4. Не автоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

6.5. При отсутствии технологической возможности осуществления не автоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

6.6. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению 4 к настоящему Положению.

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

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

6.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (сотрудники Диспансера или лица, осуществляющие такую обработку по договору), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки путем подписания уведомления по форме согласно утвержденной главным врачом.

7. Ответственность

7.1. За несанкционированное разглашение конфиденциальной информации, неправомерное использование которой может нанести материальный и моральный ущерб Диспансеру либо деловым партнерам и гражданам, на виновное должностное лицо либо сотрудника Диспансера в соответствии с Трудовым кодексом РФ может быть наложено дисциплинарное взыскание (вплоть до увольнения), а также взысканы убытки согласно ст. 139 Гражданского кодекса РФ. Кроме того, виновное должностное лицо или служащий администрации может быть привлечено в установленных законом случаях к административной ответственности (статья 13.14 Кодекса об административных правонарушениях), а также к уголовной ответственности (статьи 155, 183 Уголовного кодекса РФ).