Утверждаю:
Главный врач ГБУЗ «Областной наркологический диспансер»
_____ Г.В. Ефименко
«10» 01 2016г.

Положение о защите персональных данных при их обработке в информационных системах

1. Предмет положения о защите персональных данных

Данное положение утверждается приказом главного врача ГБУЗ «Областной наркологический диспансер».

Предметом данного положения являются порядок получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, обрабатываемых в ГБУЗ «Областной наркологический диспансер».

Положение основывается на документах, которые регламентируют требования к процессам обращения с персональными данными, в том числе и в медицинских учреждениях. К этим документам относятся:

- Конституция Российской Федерации, принятая 12.12.1993г., с поправками от 30.12.2008г., 05.02.2014г. и 21.07.2014г.; ст. 23, 24 (неприкосновенность частной жизни, личная и семейная тайна), ст. 41, 42 (недопустимость сокрытия информации, связанной с угрозой жизни и здоровью);
- федеральный закон «Об основах охраны здоровья граждан в Российской Федерации № 323-ФЗ от 21.11.2011г., в ст. 13 дано определение врачебной тайны как "информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении";
- федеральный закон '"Об информации, информационных технологиях и защите информации" № 149-ФЗ от 27.07.2006г. с внесенными изменениями Федеральным закононом от 02.07.2013г. № 187-ФЗ. Законом определяются понятия: информация, документирование информации, защита информации, обладатель информации, конфиденциальность информации, предоставление и распространение информации, электронное сообщение и др.;
- федеральный закон "О персональных данных" № 152-ФЗ от 27.07.2006 с внесенными изменениями федеральным законом от 25.07.2011г. № 261-ФЗ, от 05.04.2013г. № 43-ФЗ, 21.07.2014г. № 242-ФЗ (далее — Закон), которым регулируются отношения, связанные с обработкой персональных данных с использованием средств автоматизации;
- указ Президента РФ "Об утверждении перечня сведении конфиденциального характера" № 188 от 06.03.1997г. (в редакции указа Президента РФ от 23.09.2005 № 1111, внесены изменения Указом Президента РФ от 13.07.2015г. № 357) в котором к указанной категории сведений отнесены персональные данные и сведения, содержащие врачебную тайну;
- указ Президента РФ № 351 от 17.03.2008г. (с внесенными изменениями Указом Президента РФ от 22.05.2015г. № 260) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

постановление Правительства РФ № 687 от 15.09.2008 "Об утверждении

положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

2. Основные определения и понятия, используемые в области защиты персональных данных

Далее перечислены основные понятия, которые используются при работе с персональными данными:

- **персональные данные** (далее ПД) - 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 и другая информация;
- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие сбор и обработку персональных данных, а также определяющие цели и содержание обработки 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;
- **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;
- **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
- **трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу

власти иностранного государства, физическому или юридическому лицу иностранного государства;

общедоступные **персональные данные** - персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

3. Цель и задачи ГБУЗ «Областной наркологический диспансер» в области получения и обработки персональных данных

Целью получения, обработки, хранения персональных данных учреждением ГБУЗ «Областной наркологический диспансер» являются:

- оказание специализированной медицинской помощи на основании устава ГБУЗ «Областной наркологический диспансер»;
- выполнение функций отдела кадров предприятия

4. Понятие категории и класса персональных данных

Установлены следующие категории персональных данных (ПД):

- **категория 1** — ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- **категория 2** — ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;
- **категория 3** — персональные данные, позволяющие идентифицировать субъекта ПД;
- **категория 4** — обезличенные и (или) общедоступные персональные данные.

Информационные системы персональных данных подразделяются на типовые и специальные. К типовым системам относятся системы, в которых требуется обеспечить только конфиденциальность персональных данных. Все остальные системы относятся к специальным информационным системам.

В зависимости от последствий нарушений заданной характеристики безопасности персональных данных типовой информационной системе присваивается один из классов:

- **класс 1 (К1)** — информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;
- **класс 2 (К2)** — информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;
- **класс 3 (К3)** — информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;
- **класс 4 (К4)** — информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

Класс типовой информационной системы определяется оператором в соответствии с таблицей, приведенной в Приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20.

Кроме того, имеет значение объем обрабатываемых персональных данных, который можно условно разделить на три группы:

- менее 1000 субъектов или в пределах организации

- от 1000 до 100000 субъектов ПД или в пределах отрасли экономики, органе государственной власти или проживающих в пределах муниципального образования
- более 100000 субъектов ПД или в пределах Российской Федерации

5. Персональные данные, обрабатываемые в ГБУЗ «Областной наркологический диспансер»

ГБУЗ *«Областной наркологический диспансер» получает, обрабатывает и хранит* следующие персональные данные:

- Фамилия, имя, отчество пациента; дата, место рождения
- Паспортные данные
- Диагноз, история болезни

6. Модели угроз при обработке персональных данных

- Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.)
- Угрозы социально-политического характера: забастовки, саботаж, локальные конфликты и т.д.
- Ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз. Если, например, в качестве объекта угроз выступает автоматизированная система в защищенном исполнении (АСЗИ), то к таким действиям и нарушениям, в частности, относятся:
  - Непредумышленное искажение или удаление программных компонентов АСЗИ
  - Внедрение и использование неучтенных программ
  - Игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации

В частности:

- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа
- Угрозы техногенного характера, основными из которых являются:
  - Аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);
  - Неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;

Помехи и наводки, приводящие к сбоям в работе аппаратных средств.

7. **Мероприятия оператора, направленные на защиту персональных данных**

Оператор при обработке персональных данных **обязан:**

- принимать необходимые организационные и технические меры, в том числе

использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

- проводить мероприятия, направленные на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременно обнаруживать факты несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- предусматривать возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществлять постоянный контроль над уровнем защищенности персональных данных.

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

При обработке персональных данных в информационной системе должно быть обеспечено:	**Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:**
а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;	а) определение угрозбезопасности персональных данных при их обработке, формирование на их основе модели угроз
б) своевременное обнаружение фактов несанкционированного доступа к персональным данным	б) 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
в)недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их фун	в) проверку готовности средства защиты информации к использованию с составлением заключений о возможности их эксплуатации
г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией
д) постоянный контроль за обеспечением уровня защищенности персональных данных	д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними
	е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных
	ж) учет лиц, допущенных к работе с персональными данными в информационной системе
	з) контроль за соблюдением условий использовакния средств защиты информации, предусмотренных эксплуатационной и технической документацией

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений
к) описание системы защиты персональных данных