

«УТВЕРЖДАЮ»

И. о. главного врача ГАУЗ «КККВД»



Ю.А. Михайлова

2015г.

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСУДАРСТВЕННОГО
АВТОНОМНОГО УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ «КРАЕВОГО
КЛИНИЧЕСКОГО КОЖНО-ВЕНЕРОЛОГИЧЕСКОГО
ДИСПАНСЕРА»

1. Общие положения

1.1. Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - 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.

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.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2. Назначение и правовая основа документа

Политика государственного автономного учреждения здравоохранения «краевого клинического кожно-венерологического диспансера» (далее учреждение) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Учреждение в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Учреждения позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. Объекты защиты

Основными объектами системы безопасности персональных данных в Учреждении являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные;
- процессы обработки персональных данных в информационной системе персональных данных Учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

3. Цели и задачи обеспечения безопасности персональных данных

3.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных Учреждения являются:

- Учреждение, как собственник информационных ресурсов;
- руководство и сотрудники Учреждения, в соответствии с возложенными на них функциями;
- физические лица, состоящие с Учреждением в гражданско-правовых отношениях (граждане);

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

3.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Учреждения от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Учреждения, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Учреждения и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.
- Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

4. Основные принципы построения системы безопасности персональных данных

При обработке персональных данных пациентов Учреждение придерживается принципов:

- добросовестности и законности целей и способов обработки персональных данных;
- соблюдения законности получения, обработки, хранения, а также других действий с персональными данными;
- соответствия объема и содержания обрабатываемых персональных данных и способов обработки персональных данных целям обработки;
- достоверности персональных данных, их актуальности и достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- ограничения обработки персональных данных при достижении конкретных и законных целей, запрета обработки персональных данных, несовместимых с целями сбора персональных данных;
- осуществления хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен действующим законодательством. Персональные данные подлежат уничтожению или обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

5. Обеспечение информационной безопасности

Обеспечение безопасности персональных данных в Учреждении достигается следующими мерами:

- назначением работника, ответственного за организацию обработки персональных данных;
- проведением внутреннего аудита информационной системы организации, содержащей персональные данные, проведением их классификации;
- разработкой частной модели угроз безопасности персональных данных;
- определением списка лиц, допущенных к работе с персональными данными;
- разработкой и утверждением локальных нормативных актов организации, регламентирующих порядок обработки персональных данных. Разработкой для администраторов информационной системы рабочих инструкций;
- реализацией технических мер, снижающих вероятность реализаций угроз безопасности персональных данных;

- проведением периодических проверок состояния защищенности информационной системы организации.

6. Передача персональных данных третьим лицам

Передача персональных данных третьим лицам возможна в исключительных случаях только с письменного согласия пациента, кроме случаев, когда такая обязанность у Учреждения наступает в результате требований федерального законодательства.

7. Права субъектов персональных данных

В соответствии с Федеральным Законом № 152-ФЗ «О персональных данных» субъект персональных данных имеет право:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых Обществом и источник их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- иные права, предусмотренные действующим законодательством Российской Федерации.

Соответствующая информация предоставляется субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен быть составлен в соответствии с требованиями законодательства.