Приложение 3
к Приказу № 168.1п от 28.03.2013 г.

УТВЕРЖДАЮ

Главный врач ММАУ «Городская поликлиника №14»

_____ **О.А. Костоломова**

«___» _____ 2013 г.

ПОЛИТИКА

обработки и защиты персональных данных в информационных системах персональных данных ММАУ «Городская поликлиника №14»

2013 г.

Оглавление

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы

(уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным

лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), 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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

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.

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.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС – антивирусные средства

АРМ– автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

Введение

Настоящая Политика обработки и защиты персональных данных (далее – Политика) в ММАУ «Городская поликлиника №14» является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

В политике определены цели и задачи в области обработки и защиты персональных данных, категории субъектов, персональные данные которых обрабатываются в ИСПДн Учреждения, виды персональных данных, условия их обработки и передачи третьим лицам, основания для их обработки, принципы защиты и процедура доступа субъектов к своим персональным данным.

1. Общие положения

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных (далее – ПДн) субъекта ПДн (далее – Субъект), которые обрабатываются в ИСПДн ММАУ «Городская поликлиника №14» (далее – Учреждение), расположенного по адресу: г. Тюмень, ул. Широтная, 23а и являющегося оператором персональных данных.

1.2. Целью настоящей Политики является предоставление субъектам персональных данных, обрабатываемых в Учреждении, информации, касающейся принципов, способов и условий обработки и защиты персональных данных в Учреждении.

1.3. Политика распространяется на ПДн, полученные как до, так и после подписания настоящей Политики.

2. Цели в области обработки и защиты персональных данных

ИСПДн «Бухгалтерский и кадровый учет»: ведение учета сотрудников Учреждения, формирование отчетности, начисление заработной платы.

ИСПДн «Медицинская часть»: медицинский учет пациентов Учреждения, реализация программы ОМС.

3. Категории субъектов, персональные данные которых обрабатываются в ИСПДн Учреждения

ИСПДн «Бухгалтерский и кадровый учет»: сотрудники Учреждения.

ИСПДн «Медицинская часть»: граждане РФ, получающие медицинские услуги в Учреждении.

4. Виды персональных данных, обрабатываемых в информационных системах персональных данных Учреждения

ИСПДн «Бухгалтерский и кадровый учет»:

- ФИО;
- Пол;
- Гражданство;
- Дата рождения;
- Место рождения;
- Паспортные данные;
- Адрес места регистрации;
- Адрес места жительства;

- Контактный телефон;
- Семейное положение;
- Состав семьи;
- Сведения о воинском учете;
- № страхового полиса;
- ИНН;
- СНИЛС;
- Образование;
- Профессия/стаж;
- Должность;
- Место работы;
- Период работы;
- Специальность по диплому;
- Размер заработной платы;
- № диплома;
- Социальные льготы;
- Отпуска, больничные, повышения квалификации.

ИСПДн «Медицинская часть»:

- ФИО;
- дата рождения;
- адрес места жительства;
- контактный телефон;
- номер страхового полиса;
- диагноз;
- данные о смерти;
- семейное положение;
- лекарственный рецепт.

5. Условия обработки персональных данных и их передачи третьим лицам

5.1. Учреждение вправе передать третьим лицам в следующих случаях:

5.1.1. Субъект явно выразил свое согласие на такие действия;

5.1.2. Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры;

5.2. При обработке персональных данных Субъекта Учреждение руководствуется Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и настоящей Политикой.

5.3. Учреждение вправе передать ПДн Работника третьим лицам в случаях, предусмотренных законодательство Российской Федерации.

5.4. При обработке персональных данных Работника Учреждение руководствуется Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и настоящей Политикой.

5.5. Длительность хранения ПДн субъекта идентична длительности выполнения работ и срокам обозначенным федеральным законодательством РФ и иными нормативно-правовыми актами РФ и составляет - 75 лет.

6. Основания для обработки персональных данных

Обработка персональных данных осуществляется, руководствуясь:

6.1. Конституцией Российской Федерации, принятой 12.12.1993;

6.2. Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

6.3. Статьями 85-90 Трудового кодекса Российской Федерации (Федерального закона от 30.12.2001 г. № 197-ФЗ);

6.4. Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 28.12.2013) «Об основах охраны здоровья граждан в Российской Федерации».

7. Использование и обработка персональных данных

7.1. Персональные данные Субъекта используются исключительно в целях, обозначенных в настоящей политике путем их автоматизированной обработки, а также без использования средств автоматизации.

8. Защита персональных данных

1. Защита персональных данных осуществляется путем проведения организационно-технических мероприятий в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, приказом ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятых в соответствии с ним нормативно-правовыми актами, операторами, являющимися

государственными или муниципальными органами» и другими нормативно-правовыми актами и локальными нормативными актами Учреждения.

9. Доступ субъекта к своим персональным данным

9.1. Субъект имеет право на получение информации, касающейся обработки его персональных данных на основании письменного заявления.

9.2. Заявления принимаются по адресу:

- ул. Широтная, 23а (телефон 39-22-88).

9.3. Лицо ответственное за организацию обработки персональных данных в Учреждении – медицинский статистик Хохлова Альбина Нифантовна.

10. Для выполнения политики реализуются следующие задачи

10.1. Поддержание результативного функционирования системы обработки и защиты персональных данных.

10.2. Совершенствование локальной нормативной базы, регламентирующей порядок обработки и защиты персональных данных.

10.3. Предотвращение случаев несанкционированного доступа к персональным данным.

10.4. Внедрение современных методов для обеспечения защиты персональных данных.

10.5. Проведение организационных и технических мероприятий, направленных на совершенствование системы обработки и защиты персональных данных.

11. Принципы реализации политики в области обработки и защиты персональных данных

11.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

11.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями, описанными в настоящей Политике.

11.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

11.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

11.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

11.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Обеспечение принятия необходимых мер по удалению или уточнению неполных или неточных данных.

12. Изменение политики

12.1. Учреждение имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента её подписания, если иное не предусмотрено новой редакцией Политики.

12.2. Действующая редакция хранится в месте нахождения исполнительного органа Учреждения по адресу: г. Тюмень, ул. Широтная, 23а, ММАУ «Городская поликлиника №14» (телефон 39-22-88).