Приложение 3
к Приказу № 20
от «16» июня 2014 г.

УТВЕРЖДАЮ

Директор ООО «ЦСМ ВЕРА»

_____ Девятковская С.А.

«16» июня 2014 г.

ПОЛИТИКА

обработки и защиты персональных данных в информационных системах персональных данных Общества с ограниченной ответственностью «Центр Семейной Медицины ВЕРА»

2014 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 информации (в том числе персональных данных) – состояние защищенности информации (в том числе персональных данных), характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации (в том числе персональных данных) при их обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки (за исключением случаев, если обработка необходима для уточнения информации, в том числе 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.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – одно из важнейших свойств системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

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.

Информация – сведения (сообщения, данные) независимо от формы их представления, в том числе в следующем виде:

- записей в памяти компьютеров, электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.), обеспечивающих функционирование объекта информатизации (сети);
- сообщений, передаваемых по сетям передачи данных;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, представляемого непосредственно на экранах дисплеев, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, бумага для распечатки и т.п.) или через сети передачи данных;
- электронных записей о субъектах прав.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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 информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней;

Лицензия **на право оказания услуг** в области защиты информации - разрешение на право проведения тех или иных работ в области защиты информации;

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.

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.

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).

Пользователь информационной системы– лицо, участвующее в функционировании информационной системы 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

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.

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

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

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.

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 – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию) в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

БД – база данных

ИС – информационная система

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

МЭ – межсетевой экран

НСД – несанкционированный доступ

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – система (подсистема) защиты информации

СрЗИ – средство защиты информации

ТС – техническое средство

Введение

Настоящая Политика обработки и защиты персональных данных (далее – Политика) в Обществе с ограниченной ответственностью «Центр Семейной Медицины ВЕРА» (далее – Организация) является официальным документом.

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

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 Организации, 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 Организации, являющегося оператором персональных данных и расположенного по адресу: 625000, г. Тюмень, ул. Грибоедова, дом 6, корпус 1/3.

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

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

2. Цели в области обработки и защиты персональных данных

Для ПДн сотрудников - ведение учета сотрудников Организации, формирование отчетности, расчёт и начисление заработной платы.

Для ПДн получателей медицинских услуг – регистрация и учет пациентов, ведение истории болезни, расчетные операции.

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

Категории субъектов, ПДн которых обрабатываются в Организации:

- сотрудники Организации;
- получатели медицинских услуг.

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

Данные о сотрудниках (иные категории ПДн):

- ФИО;
- пол;
- гражданство;
- дата рождения;
- место рождения;
- серия и номер паспорта, дата и место его выдачи;
- адрес места регистрации;
- адрес места жительства;
- контактный телефон;
- семейное положение;

- состав семьи;
- ИНН;
- СНИЛС;
- лицевой банковский счет (зарплатный);
- образование;
- профессия/стаж;
- должность;
- место работы;
- период работы;
- специальность по диплому;
- размер заработной платы;
- номер диплома;
- социальные льготы;
- отпуска, больничные, повышения квалификации;
- сведения о заработной плате.

Данные о получателях услуг (специальные категории):

- ФИО;
- пол;
- дата рождения;
- серия и номер паспорта, дата и место его выдачи;
- адрес места регистрации;
- адрес места жительства;
- контактный телефон;
- номер страхового полиса;
- СНИЛС;
- социальное положение;
- должность;
- место работы;
- диагноз;
- данные о здоровье.

5. Условия обработки персональных данных и их передачи третьим лицам

5.1. Организация 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 Организация руководствуется Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и настоящей Политикой.

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

5.4. При обработке персональных данных Работника Организация 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, для ПДн сотрудников – 75 лет (срок хранения карточек работников), для ПДн получателей медицинских услуг – 5 (срок хранения медицинской карты амбулаторного больного).

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 № 152-ФЗ «О персональных данных»;

6.3. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;

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

7. Использование и обработка персональных данных

7.1. Персональные данные Субъекта используются исключительно в целях, обозначенных в настоящей политике посредством их автоматизированной обработки, а также посредством обработки, осуществляемой 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 № 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 Организации.

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:

- 625000, г. Тюмень, ул. Грибоедова, дом 6, корпус 1/3 (телефон (3452) 685-904 доб. 446).

9.3. Лицо ответственное за организацию обработки персональных данных в Организации – Шалемов Владимир Михайлович, заместитель директора по АХЧ.

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 Организации по адресу: 625000, г. Тюмень, ул. Грибоедова, дом 6, корпус 1/3 (телефон (3452) 685-904 доб. 446)