УТВЕРЖДАЮ

Главный врач МБУЗ «ЦГБ»

_____ Ю.А. Медин

«___» _____ 201__ г.

Политика информационной безопасности

информационных систем персональных данных

МБУЗ «ЦГБ» г. Донецка

СОДЕРЖАНИЕ

Определения.....3

Обозначения и сокращения.....9

1 Общие положения.....10

2 Категории персональных данных, обрабатываемых в учреждении.....10

3 Правовые основания обработки персональных данных.....14

4 Цели обработки персональных данных.....11

5 Принципы обработки персональных данных в учреждении.....12

6 Меры по обеспечению защиты персональных данных в учреждении.....13

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 сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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 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.

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких 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, сопровождающих 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 невозможно определить принадлежность персональных данных конкретному субъекту 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.

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, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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.

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

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, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки — электромагнитые 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 осуществит утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (ил) 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 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.

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 разграниченного доступа.

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 оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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 невозможно восстановить содержание персональных данных в информационной системе персональных данных 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 доступности

ОС — операционная системами

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 — средства защиты персональных данных

СОВ — система обнаружения вторжений

ТКУИ — технические каналы утечки информации

УБПДн — угрозы безопасности персональных данных

1. Общие положения

Политика обработки персональных данных в Муниципальном бюджетном учреждении здравоохранения «Центральная городская больница» (далее – Политика) разработана во исполнение требований Федерального закона РФ 2006 г. № 152-ФЗ «О персональных данных».

Политика определяет:
- категории персональных данных, обрабатываемых в МБУЗ «ЦГБ» (далее – учреждение);
- правовые основания обработки персональных данных;
- цели обработки персональных данных;
-принципы обработки персональных данных;
- меры по обеспечению защиты персональных данных в учреждении.

Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в учреждении вопросы обработки персональных данных работников учреждения и других субъектов персональных данных.

Изменения в Политику вносятся на основании приказов руководителя учреждения.

2. Категории персональных данных, обрабатываемых в учреждении

2.1 В учреждении обрабатываются:

персональные данные работников учреждения;

персональные данные граждан, застрахованных по обязательному медицинскому страхованию;

специальные категории персональных данных о состоянии здоровья, в том числе – диагноз, код заболевания по международному классификатору болезней (МКБ10), факт обращения за медицинской помощью;

персональные данные экспертов качества медицинской помощи, включенных в территориальный реестр экспертов качества медицинской помощи в сфере обязательного медицинского страхования Ростовской области;

персональные данные медицинских работников, включенных в региональный сегмент Федерального регистра лиц, участвующих в оказании медицинских услуг;

персональные данные физических лиц, содержащиеся в сведениях о государственной регистрации смерти.

Источниками персональных данных, обрабатываемых в учреждении, являются:

Федеральный фонд обязательного медицинского страхования;

территориальные фонды обязательного медицинского страхования других субъектов Российской Федерации;

медицинские и страховые организации, осуществляющие деятельность в сфере обязательного медицинского страхования на территории Ростовской области;

Отделение Пенсионного фонда Российской Федерации по Ростовской области;

Ростовское региональное отделение Фонда обязательного социального страхования Российской Федерации;

органы записи актов гражданского состояния муниципальных районов и городских округов Ростовской области;

работники, заключившие с учреждением трудовые договоры;

организации, общественные объединения, орган исполнительной власти Ростовской области, подающие ходатайство о включении врача-специалиста в территориальный реестр экспертов качества медицинской помощи.

3. Правовые основания обработки персональных данных

Обработка персональных данных в учреждении производится на основании следующих нормативных документов:

Федеральный закон 2006 года № 152-ФЗ «О персональных данных»;

Федеральный закон 2010 года № 326-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Федеральный закон 1997 года № 143-ФЗ «Об актах гражданского состояния»;

Федеральный закон 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»;

Федеральный закон 1996 года № 61-ФЗ «Об обороне»;

Постановление Правительства Российской Федерации 2014 года № 1273 «О программе государственных гарантий бесплатного оказания гражданам медицинской помощи на 2015 года и на плановый период 2016 и 2017 годов»;

Приказ Министерства здравоохранения и социального развития Российской Федерации 2011 года № 15н «Об утверждении типового положения о территориальном фонде обязательного медицинского страхования»;

Постановление Правительства Ростовской области 2012 года № 17 «О территориальном фонде обязательного медицинского страхования Ростовской области».

4. Цели обработки персональных данных

Обработка персональных данных в учреждении осуществляется с целью:

реализации государственной политики в области обязательного медицинского страхования на территории Ростовской области;

обеспечения всеобщности обязательного медицинского страхования граждан;

достижения социальной справедливости и равенства всех граждан в системе обязательного медицинского страхования;

обеспечения финансовой устойчивости системы обязательного медицинского страхования;

ведения учета застрахованных по обязательному медицинскому страхованию граждан на территории Ростовской области;

контроля качества, объемов, сроков, условий оказанной медицинской помощи;

контроля за рациональным использованием финансовых средств, направляемых на обязательное медицинское страхование на территории Ростовской области;

исполнения налогового законодательства, законодательства по воинскому учету, социальному обеспечению, социальному страхованию;

ведения кадровой работы.

5. Принципы обработки персональных данных в учреждении

Обработка персональных данных в учреждении основана на следующих принципах:

законность;

соответствие целей обработки персональных данных полномочиям учреждения;

недопустимость обработки персональных данных для целей, несовместимых с целями сбора персональных данных;

недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки;

обеспечение точности, достаточности, а в необходимых случаях и актуальности персональных данных;

хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо

обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

6. Меры по обеспечению защиты персональных данных в учреждении

Для обеспечения защиты персональных данных в учреждении приняты следующие меры:

назначен ответственный сотрудник за организацию обработки персональных данных в учреждении;

организован учет машинных носителей информации, используемых для работы с персональными данными;

используются криптографические средства защиты информации, сертифицированные ФСБ России, а также программные и программно-аппаратные средства защиты информации от несанкционированного доступа, сертифицированные ФСТЭК России.

Руководителем учреждения утверждены следующие документы:

Положение по организации работ с персональными данными в учреждении;

Модель угроз и нарушителя безопасности персональных данных в учреждении;

Инструкции пользователя информационной системы персональных данных;

Список опечатываемых помещений, в которых обрабатываются персональные данные;

Перечень работников учреждения, имеющих доступ к персональным данным;

Инструкция по организации парольной защиты в учреждении;

Инструкция по организации антивирусной защиты в учреждении.

6.3 Сведения об учреждении внесены в Реестр операторов, осуществляющих обработку персональных данных (регистрационный номер СФ/111-1856, дата внесения «17» июня 2012 г.).