Приложение 1 к прик. №141

УТВЕРЖДАЮ

Главный врач ГБУЗ ТО
«ДПН ЛРЦ «Надежда»

_____ Кашуба Е.В.

«15» июня 2015 г.

ПОЛИТИКА

обработки и защиты персональных данных в ГБУЗ ТО «ДПН ЛРЦ «Надежда»

2015г.

Оглавление

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических 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 втайне от субъектов, не имеющих полномочий на право доступа к ней.

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.

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

Представитель Субъекта персональных данных – законный представитель субъекта:

- лицо, выступающее на основании доверенности, удостоверенной в установленном порядке.

- опекун, попечитель с представлением подтверждающего документа;
- родители несовершеннолетнего до 18 лет.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

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

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

Субъект персональных данных (Субъект) – резиденты РФ; физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором).

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.

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).

Введение

Настоящая Политика обработки и защиты персональных данных (далее – Политика) в ГБУЗ ТО «ДПН ЛРЦ «Надежда» (далее – Учреждение) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Положении об обработке и защите персональных данных Учреждения.

В Политике определены цели и обработки персональных данных, категории Субъектов персональных данных, чьи персональные данные обрабатываются в Учреждении, категории и состав 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 Субъектов, которые обрабатываются в Учреждении.

1.2. Учреждение является оператором персональных данных и расположено по адресу: 625000, Российская Федерация, город Тюмень, улица Хохрякова 80/1.

1.3. Целью настоящей Политики является предоставление Субъектам персональных данных, чьи персональные данные обрабатываются в Учреждении, информации, касающейся принципов, способов и условий обработки и защиты персональных данных в Учреждении.

1.4. Политика распространяется на персональные данные, полученные как до, так и после подписания настоящей Политики.

2. Категории субъектов персональных данных

В Учреждении обрабатываются персональные данные, принадлежащие следующим категориям Субъектов:

- пациенты (граждане Российской Федерации и лица без гражданства РФ);
- сотрудники Учреждения.

3. Цели обработки персональных данных

Цели обработки персональных данных в Учреждении:

- для персональных данных пациентов – оказание медицинских услуг в соответствии с законодательством РФ;
- для персональных данных сотрудников– ведение кадрового и бухгалтерского учета сотрудников Учреждения, формирование отчетности, расчёт и начисление заработной платы.

4. Основание обработки персональных данных

Основание для обработки персональных данных:

- Конституция Российской Федерации, от 12.12.1993;
- Гражданский кодекс РФ от 20.11.1994 (Федеральный закон от 30.11.1994 № 51-ФЗ);
- ст.ст. 85-90 Трудового кодекса Российской Федерации (Федерального закона от 30.12.2001 № 197-ФЗ);

- ст. 23, 24, 41, 42 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- гл. 10 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. от 23.09.2005 № 1111);
- Устав ГБУЗ ТО «ДПН ЛРЦ «Надежда».

5. Категории и состав обрабатываемых персональных данных

Персональные данные пациентов (*специальные категории персональных данных субъектов, не являющихся сотрудниками оператора*):

- ФИО;
- дата рождения;
- адрес места жительства;
- контактный телефон;
- номер страхового полиса;
- диагноз;
- лекарственный рецепт;
- сведения о здоровье.

Персональные данные сотрудников (*иные категории персональных данных сотрудников оператора*):

- 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;
- Сведения о заработной плате.

6. Сроки обработки и хранения персональных данных

6.1. Сроки обработки и хранения персональных данных Субъекта соответствуют длительности выполнения работ и срокам, обозначенным федеральным законодательством РФ и иными нормативно-правовыми актами РФ.

6.2. Сроки обработки и хранения персональных данных пациентов – 25 лет (соответствует сроку хранения первичных медицинских документов).

6.3. Сроки обработки и хранения персональных данных сотрудников – 75 лет (соответствует сроку хранения личных дел работников, основание – Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утв. Росархивом 06.10.2000).

7. Условия обработки и передачи персональных данных третьим лицам

7.1. Обработка вышеуказанных персональных данных осуществляется смешанным путем: автоматизированная обработки персональных данных (с использованием ПЭВМ), с передачей полученной информации по внутренней (локальной) сети организации, и с использованием сети общего пользования Интернет по защищённым каналам связи, а также неавтоматизированная обработка.

7.2. Действия, совершаемые с персональными данными при их обработке: сбор, запись, систематизация, накопление, хранение, уточнение (изменение), использование, передача (предоставление), обезличивание, удаление.

7.3. Учреждение вправе передать персональные данные третьим лицам в следующих случаях:

7.3.1. Субъект персональных данных явно выразил свое согласие на такие действия;

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

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

7.5. При обработке персональных данных Субъекта трансграничная передача персональных данных не ведётся.

8. Принципы обработки персональных данных

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

8.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

8.5. 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.

8.6. 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. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

8.7. Хранение персональных данных должно осуществляться 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 федеральным законом.

8.8. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять

персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом.

9. Меры по обеспечению безопасности персональных данных при их обработке

В Учреждении принимаются следующие меры по обеспечению безопасности персональных данных при их обработке:

1) назначен работник, ответственный за организацию обработки персональных данных;
2) изданы документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
3) осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
4) проведена оценка вреда, который может быть причинен Субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
5) проведено ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
6) обеспечивается принятие необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7) определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
8) применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
9) применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
10) ведётся учет машинных носителей персональных данных;
11) ведётся обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
12) ведётся восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
13) установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
14) ведётся контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10. Права субъекта персональных данных[1]

10.1. Субъект персональных данных имеет право на получение от Оператора, обрабатывающего его персональные данные, следующих сведений:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему Субъекту персональных данных, источник их

[1] За основу приведённых в настоящем разделе пунктов взяты положения ст.ст. 14, 17 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления Субъектом персональных данных прав, предусмотренных ФЗ-152 «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ-152 «О персональных данных» или другими федеральными законами.

10.2. Субъект персональных данных имеет право:

- требовать от Оператора 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;
- принимать предусмотренные законом меры по защите своих прав.

10.3. Субъект персональных данных имеет право доступа к своим персональным данным:

- при личном обращении к представителю Оператора;
- при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность Субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие факт обработки персональных данным Оператором (номер договора, дата заключения договора, условное словесное обозначение и(или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором и собственноручную подпись Субъекта персональных данных. Запрос может быть направлен в форме электронного документа и подписан электронной подписью;
- в случае, если сведения, указанные в пункте 1.2., а также обрабатываемые персональные данные, были предоставлены для ознакомления Субъекту персональных данных по его запросу, Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях ознакомления со сведениями, указанными в части 1.2., и

ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, нормативным правовым актом или договором.

10.4. Право Субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание Субъекта персональных данных по подозрению в совершении преступления, либо предъявившими Субъекту персональных данных обвинение по уголовному делу, либо применившими к Субъекту меру пресечения, до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

10.5. Если Субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований ФЗ-152 «О персональных данных» или иным образом нарушает его права и свободы, Субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

10.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

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

10.8. Заявления от Субъектов персональных данных принимаются по адресу: 625000, Российская Федерация, город Тюмень, улица Хохрякова 80/1 (телефон (3452) 25-72-95).

10.9. Лицо, ответственное за организацию обработки персональных данных в Учреждении – Кашуба Е.В., Заместитель Главного врача по ОМР.

11. Изменение политики

11.1. 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.

11.2. Действующая редакция хранится в месте нахождения исполнительного органа Учреждения по адресу: 625000, Российская Федерация, город Тюмень, улица Хохрякова 80/1(телефон (3452) 25-72-95).