

Государственное бюджетное учреждение здравоохранения Самарской области
«Шенталинская центральная районная больница»

ПРИКАЗ

«01» НОЯБРЯ 2018г.

№ 236

«О назначении ответственного за организацию обработки персональных данных
и об утверждении политики в отношении обработки персональных данных
ГБУЗ СО «Шенталинская ЦРБ»

В целях исполнения требований Федерального закона от 27.07.2006г. №152 «О персональных данных» п.п.2 п.1 ст.18.1 и постановления Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в ГБУЗ СО «Шенталинская ЦРБ» ведущего инженера-программиста Дементьеву А.В.
2. Утвердить политику в отношении обработки персональных данных ГБУЗ СО «Шенталинская ЦРБ» (Приложение №1).
3. Ведущему инженеру-программисту Дементьевой А.В. опубликовать приказ на официальном сайте ГБУЗ СО «Шенталинская ЦРБ».
4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач
ГБУЗ СО «Шенталинская ЦРБ»



В.В. Михайлов

Согласовано:

Ведущий инженер-программист



А.В. Дементьева

Программист



А.Ю. Трофимов

Главная медицинская сестра



Л.Г. Морозова

Юрисконсульт



Е.А. Колточник

УТВЕРЖДАЮ
Главный врач ГБУЗ СО «Шенталинская ЦРБ»
В.В. Михайлов
2018 г.

ПОЛИТИКА **в отношении обработки персональных данных** **государственного бюджетного учреждения здравоохранения** **Самарской области «Шенталинская центральная районная больница»**

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» в отношении обработки персональных данных в ГБУЗ СО «Шенталинская ЦРБ» (далее - Учреждение) и действует в отношении персональных данных, которые Учреждение получило и может получить от субъектов персональных данных (далее – ПДн).

1.2. При обработке ПДн Учреждение руководствуется законодательством Российской Федерации, в том числе:

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

1.2.2. Постановлением Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.2.3. Постановлением Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»;

1.2.4. Приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Основные понятия, используемые в Политике:

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

1.3.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средства автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

1.3.3. 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;

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

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

1.4. Политика является основным руководящим документом Учреждения, определяющим требования, предъявляемые к обеспечению безопасности ПДн.

1.5. Целью Политики является обеспечение безопасности ПДн, а также реализация положений нормативных правовых актов и иных документов по защите ПДн в соответствии с законодательством РФ.

1.6. Основными целями обеспечения безопасности персональных данных являются:

1.6.1. Предотвращение нарушений прав субъекта ПДн (физического лица) и сохранение конфиденциальности информации, обрабатываемой в ИСПДн Учреждения;

1.6.2. Предотвращение искажения или несанкционированной модификации информации, содержащей ПДн, обрабатываемой в ИСПДн Учреждения;

1.6.3. Предотвращение несанкционированных действий по блокированию информации, содержащей ПДн.

1.7. Обработка ПДн осуществляется с целью:

1.7.1. Оказания медицинских услуг;

1.7.2. Исполнения условий трудового договора и осуществления прав и обязанностей в соответствии с трудовым законодательством;

1.7.3. Принятия решения о трудоустройстве;

1.7.4. Принятия решений по обращениям граждан Российской Федерации в соответствии с законодательством.

1.8. Обработка ПДн в Учреждении основана на следующих принципах:

1.8.1. Осуществления на законной и справедливой основе;

1.8.2. Соответствия целей обработки ПДн полномочиям Учреждения;

1.8.3. Соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;

1.8.4. Достоверности ПДн, их актуальности и достаточности для целей обработки, недопустимости обработки избыточных по отношению к целям сбора ПДн;

1.8.5. Ограничения обработки ПДн при достижении законных и конкретных целей, запретом обработки ПДн, несовместимых с целями сбора ПДн;

1.8.6. Запрета объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

1.8.7. Осуществления хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен действующим законодательством.

2. Состав организационных и технических мер по обеспечению безопасности персональных данных при их обработке

2.1. Учреждение принимает необходимые и достаточные правовые, организационные и технические меры для защиты ПДн субъектов ПДн, в соответствии ст.19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ. К таким мерам, в частности, относятся:

2.1.1. Назначение сотрудника, ответственного за организацию обработки ПДн;

2.1.2. Осуществление внутреннего контроля соответствия обработки ПДн Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;

2.1.3. Ознакомление работников, непосредственно осуществляющих обработку ПДн, с положениями действующего законодательства о ПДн, требованиями к защите ПДн и иными документами по вопросам обработки ПДн;

2.1.4. Определение угроз безопасности ПДн при их обработке в ИСПДн;

2.1.5. Применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия и сертификации;

2.1.6. Осуществление оценки эффективности принимаемых мер по обеспечению безопасности ПДн;

2.1.7. Обеспечение целостности информационной системы и информации;

2.1.8. Осуществление учета машинных носителей ПДн;

- 2.1.9. Защита машинных носителей информации;
- 2.1.10. Идентификация и аутентификация субъектов доступа и объектов доступа;
- 2.1.11. Управление доступом субъектов доступа к объектам доступа;
- 2.1.12. Обеспечение доверенной загрузки в ИСПДн;
- 2.1.13. Ограничение программной среды ИСПДн;
- 2.1.14. Антивирусная защита;
- 2.1.15. Защита информационной системы, ее средств и систем связи и передачи данных;
- 2.1.16. Осуществление контроля за принимаемыми мерами по обеспечению безопасности

ПДн и уровня защищенности ИСПДн;

- 2.1.17. Разработка локальных документов по вопросам обработки ПДн.

2.2. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

2.3. Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3. Особенности обработки персональных данных и их передачи третьим лицам

3.1. Обработка ПДн должна осуществляться работниками, имеющими допуск к ПДн. Данные работники обязаны соблюдать положения настоящей Политики, а также своих должностных инструкций и других документов Учреждения в области защиты ПДн.

3.2. Учреждение обрабатывает ПДн, которые получило и может получить от следующих субъектов ПДн:

3.2.1. Граждан, обращающихся в Учреждение для получения медицинских услуг;

3.2.2. Граждан, состоящих с Учреждением в отношениях, регулируемых трудовым законодательством;

3.2.3. Граждан, являющихся претендентами на замещение вакантных должностей;

3.2.4. Граждан, обращающихся в Учреждение в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

3.3. Учреждение вправе передать ПДн третьим лицам в следующих случаях:

3.3.1. Субъект ПДн выразил свое согласие на такие действия в любой форме, позволяющей подтвердить факт его получения;

3.3.2. Передача предусмотрена федеральным законодательством в рамках установленной процедуры.

3.4. Срок хранения ПДн субъекта ПДн определяется в соответствии с действующим законодательством и иными нормативными правовыми документами.

3.5. Субъект ПДн обладает правами, предусмотренными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».