|  |  |
| --- | --- |
|  | Приложение № 1  Утверждено приказом ГБУЗ НО «Городская больница № 35» г.Н.Новгорода  от 01.09.2017 № 171-Р § 5 |

**Политика информационной безопасности**

**(далее – Политика)**

**Государственного бюджетного учреждения здравоохранения Нижегородской области «Городско больницы № 35**

**Советского района г.Нижнего Новгорода»**

**Содержание**

Основные понятия и сокращения 3

1. Общие положения 5

2. Правовые основания обработки персональных данных 7

3. Цель обработки персональных данных 8

4. Категории обрабатываемых персональных данных 9

5. Порядок и условия обработки персональных данных 10

6. Источники персональных данных 11

7. Условия прекращения обработки персональных данных 12

8. Меры по обеспечению конфиденциальности и безопасности персональных данных при их обработке в ИСПДн ГБУЗ НО «Городская больница № 35 Советсткого района г.Нижнего Новгорода» 13

8.1. Обеспечение конфиденциальности персональных данных 13

8.2. Обеспечение защиты персональных данных 13

9. Заключительные положения 15

# Основные понятия и сокращения

В настоящем документе используются следующие основные определения:

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

**Оператор персональных данных** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

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

**Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств 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.

**Распространение персональных данных** - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

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

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

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

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

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

**Субъект персональных данных -** это физическое лицо, персональные данные которого обрабатываются.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

**Персональные данные, сделанные общедоступными субъектом** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

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

**Неавтоматизированная обработка персональных данных (обработка ПДн без использования средств автоматизации)** – обработка ПДн, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого субъекта ПДн осуществляются при непосредственном участии человека. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн, либо были извлечены из нее.

# 1. Общие положения

Обработка персональных данных в Государственном бюджетном учреждении здравоохранения Нижегородской области «Городская больница №35 Советского района г.Нижнего Новгорода» (далее – ГБУЗ НО «Городская больница № 35» г.Н.Новгорода) осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в сфере защиты персональных данных и настоящей Политикой Государственного бюджетного учреждения здравоохранения Нижегородской области «Городской больницы № 35 Советского района г.Нижнего Новгорода» в отношении персональных данных (далее – Политика).

Настоящая Политика определяет общие требования:

* к обработке персональных данных работников ГБУЗ НО «Городская больница № 35» г.Н.Новгорода и лиц, обратившихся за медицинской помощью в ГБУЗ НО «Городская больница № 35» г.Н.Новгорода, застрахованных в системе обязательного медицинского страхования;
* к мерам по обеспечению защиты персональных данных.

Политика разработана во исполнение требований пункта 2 части 1 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и в целях:

* обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
* обеспечения соответствия законодательству Российской Федерации действий, направленных на обработку персональных данных;
* обеспечения основных направлений защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.

Основные задачи настоящей Политики:

* определение общих принципов,порядка обработки персональных данных;
* определение основных условий обработки персональных данных, способовзащиты персональных данных;
* определение прав и обязанностей операторов и субъектов персональных данных при обработке персональных данных.

Политика должна осуществляться в соответствии со следующими основными принципами:

* законности – соблюдение законодательства по защите персональных данных;
* эффективности и целесообразности – реализуемые мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом должна учитываться соразмерность затрат на обеспечение защиты и потенциальных потерь при реализации угроз;
* непрерывности функционирования системы информационной безопасности;
* совершенствования мер и средств защиты информации;
* персональной ответственности и обязательности контроля.

Требования настоящей Политики распространяются на все структурные подразделения ГБУЗ НО «Городская больница № 35» г.Н.Новгорода, в которых осуществляется обработка персональных данных***.***

# 2. Правовые основания обработки персональных данных

Обработка персональных данных в ИСПДн ГБУЗ НО «Городская больница № 35» г.Н.Новгорода осуществляется на основании:

1. Конституции РФ;
2. Трудового кодекса Российской Федерации;
3. Гражданского кодекса Российской Федерации;
4. Налогового кодекса Российской Федерации;
5. Федерального закона от 29.11.2010 № 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации" (далее – Федеральный закон от 29.11.2010 № 326-ФЗ);
6. Федерального закона от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
7. Устав ГБУЗ НО «Городская больница № 35» г.Н.Новгорода;
8. Договорами, заключаемыми между ГБУЗ НО «Городская больница № 35» г.Н.Новгорода и субъектом персональных данных.
9. Согласия на обработку персональных данных.

# 3. Цель обработки персональных данных

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей.

Цель обработки ПДн - это выполнение функций, полномочий и обязанностей, возложенных на ГБУЗ НО «Городская больница № 35» г.Н.Новгорода:

* Деятельность, которая предусмотрена законодательством об обязательном медицинском страховании и Уставом ГБУЗ НО «Городская больница № 35» г.Н.Новгорода, в том числе:

1. Осуществление персонифицированного учета сведений о застрахованных лицах и оказанной им медицинской помощи;
2. Осуществление гражданско-правовых отношений.
3. Организация кадрового учета организации, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам.
4. Ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами.
5. Исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование.
6. Заполнение первичной статистической документации в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации и федеральными законами.
7. Исполнение требований законодательства о судопроизводстве, об исполнительном производстве.

# 4. Категории обрабатываемых персональных данных

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода обрабатываются:

1. Специальные категории персональных данных, содержащих сведения о состоянии здоровья лиц и об оказанной им медицинской помощи, полученной в ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

2. Персональные данные физических лиц, состоящих с ГБУЗ НО «Городская больница № 35» г.Н.Новгорода в трудовых отношениях и их родственников.

3. Персональные данные бывших работников и кандидатов на замещение вакантных должностей, а также их родственников.

4. Персональные данные физических лиц, состоящих с ГБУЗ НО «Городская больница № 35» г.Н.Новгорода в гражданско-правовых отношениях.

Содержание и объем персональных данных соответствует целям обработки.

Обрабатываемые персональные данные, перечислены в рамках каждой из категорий и применительно к конкретным целям:

- в Модели угроз (при обработке ПДн с использованием средств автоматизации);

- в Положении о работе с персональными данными работника ГБУЗ НО «Городская больница № 35» г.Н.Новгорода и Перечне сведений конфиденциального характера в ГБУЗ НО «Городская больница № 35» г.Н.Новгорода (при обработке ПДн без использования средств автоматизации).

**5. Порядок и условия обработки персональных данных**

Обработка персональных данных в ИСПДн ГБУЗ НО «Городская больница № 35» г.Н.Новгорода осуществляется в соответствии со следующими принципами:

1. Законность обработки ПДн;

2. Прекращение обработки ПДн после достижения конкретных, заранее определенных и законных целей;

3. Недопустимость обработки ПДн, несовместимой с целями их сбора;

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

5. Осуществление обработки только тех ПДн, которые отвечают целям их обработки;

6. Соответствие содержания и объема, обрабатываемых ПДн заявленным целям их обработки;

7. Обеспечение точности, достаточности, а в необходимых случаях и актуальности ПДн по отношению к целям их обработки.

Обработка персональных данных в ИСПДн ГБУЗ НО «Городская больница № 35» г.Н.Новгорода осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения.

Обработка персональных данных в ГБУЗ НО «Городская больница № 35» г.Н.Новгорода осуществляется как с использованием средств автоматизации, так и без использования таких средств (автоматизированная и смешанная обработка персональных данных).

Реагирование на запросы и обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным определены Регламентом обработки запросов субъектов персональных данных, утвержденных приказом ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

Хранение ПДн осуществляется в базах данных, находящихся на территории Российской Федерации с использованием средств автоматизации и без использования средств автоматизации. Хранение ПДн организовано в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения не установлен Федеральным Законом, договором, стороной которого. выгодоприобретателем или поручителем, по которому является субъект ПДн.

Уничтожение либо обезличивание обрабатываемых персональных данных производиться по достижению целей их обработки, или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

**6. Источники персональных данных**

Источниками персональных данных, обрабатываемых в ИСПДн ГБУЗ НО «Городская больница № 35» г.Н.Новгорода являются:

1. Территориальный фонд обязательного медицинского страхования Нижегородской области.

2. Медицинские и страховые медицинские организации, осуществляющие деятельность в сфере обязательного медицинского страхования на территории Нижегородской области.

3. Министерство здравоохранения Нижегородской области.

4. Физические лица, состоящие с ГБУЗ НО «Городская больница № 35» г.Н.Новгорода в трудовых отношениях.

5. Физические лица, состоящие с ГБУЗ НО «Городская больница № 35» г.Н.Новгорода в гражданско-правовых отношениях.

6. Физические лица, являющиеся кандидатами на замещение вакантных должностей в ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода не несет ответственности за достоверность и актуальность ПДн, полученных от других организаций в соответствии с законодательством Российской Федерации.

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода предоставляет ПДн органам дознания и следствия и иным уполномоченным органам, по основаниям, предусмотренным действующим законодательством Российской Федерации.

# Условия прекращения обработки персональных данных

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода прекращает обработку персональных данных или обеспечивает прекращение их обработки лицом, действующим по поручению ГБУЗ НО «Городская больница № 35» г.Н.Новгорода, в случае:

1. Изменения, признания утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

2. Изменения или расторжения соглашений, заключенных ГБУЗ НО «Городская больница № 35» г.Н.Новгорода во исполнение нормативных правовых актов, на основании которых осуществляется обработка персональных данных;

3. Выявления неправомерной обработки персональных данных, осуществляемой ГБУЗ НО «Городская больница № 35» г.Н.Новгорода или лицом, действующим по поручению ГБУЗ НО «Городская больница № 35» г.Н.Новгорода;

4. Достижения цели обработки персональных данных;

5. Отзыва субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обработка персональных данных допускается только с согласия субъекта персональных данных.

Уничтожение персональных данных осуществляется в порядке и сроки, предусмотренные Федеральным законом от  24.07.2006 №152-ФЗ «О персональных данных».

# Меры по обеспечению конфиденциальности и безопасности персональных данных при их обработке в ИСПДн ГБУЗ НО «Городская больница № 35» г.Н.Новгорода

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода в целях обеспечения конфиденциальности и безопасности ПДн при их обработке в ИСПДн применяет необходимые правовые, организационные и технические меры, предусмотренные:

* Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Постановлением Правительства РФ от 01.11.2012  № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* 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»;
* Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

## 8.1. Обеспечение конфиденциальности персональных данных

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Обеспечение конфиденциальности ПДн не требуется:

* в случае обезличивания ПДн;
* в отношении общедоступных ПДн.

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода и иные лица, получившие доступ к ПДн, несут ответственность за разглашение сведений конфиденциального характера.

## 8.2. Обеспечение защиты персональных данных

ГБУЗ НО «Городская больница № 35» г.Н.Новгорода принимает все необходимые правовые, организационные и технические меры информационной безопасности для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн обрабатываемых Оператором достигается за счет:

1. Определения угроз безопасности персональных данных, при их обработке в ИСПДн;
2. Разработки на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием [методов и способов](consultantplus://offline/main?base=LAW;n=97942;fld=134;dst=100009) защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
3. Использования шифровальных (криптографических) средств;
4. Учета машинных носителей ПДн;
5. Установки и ввода в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
6. Ознакомления лиц, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите ПДн, локальными нормативными актами, по вопросам обработки персональных данных
7. Обучения лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
8. Обнаружения фактов несанкционированного доступа к ПДн и принятием мер;
9. Возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
10. Разграничение и установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн, учет лиц, допущенных к работе с ПДн;
11. Оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
12. Недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
13. Постоянного контроля за обеспечением уровня защищенности ПДн.

# 9. Заключительные положения

Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную ответственность, в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Политика действует с момента её утверждения соответствующим приказом ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

Политика может быть пересмотрена в результате изменений нормативных актов, регулирующих защиту ПДн и деятельность ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

Изменения и дополнения в Политику вносятся на основании приказа ГБУЗ НО «Городская больница № 35» г.Н.Новгорода.

**СОГЛАСОВАНО**

Системный администратор

(ответственный за информационную безопасность)

Папазян Месроп Ованесович

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«01» сентября 2017 года

**СОГЛАСОВАНО**

Юрисконсульт

Шмелева Надежда Евгеньевна

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«01» сентября 2017 года