Министерство здравоохранения Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
НАЦИОНАЛЬНЫЙ МЕДИЦИНСКИЙ
ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР КАРДИОЛОГИИ

# ПРИКАЗ

№ 169

«27» 11 2017 г. г. Москва

«Об утверждении Положения
по обработке персональных данных»

В целях обеспечения обработки персональных данных в соответствии с требованиями действующего законодательства в сфере защиты персональных данных, обеспечение безопасности персональных данных в ФГБУ «НМИЦ кардиологии» Минздрава России

ПРИКАЗЫВАЮ:

1. Утвердить Положение по обработке персональных данных (Приложение к настоящему приказу).
2. Признать утратившим силу Приказ № 17 от 22.01.2015 г.

Генеральный директор С.А. Бойцов

**УТВЕРЖДАЮ**
Генеральный директор
ФГБУ «НМИЦ кардиологии»
Минздрава России

_____ Бойцов С.А.

**Положение по обработке персональных данных**

Настоящее положение определяет политику федерального государственного бюджетного учреждения «Национальный медицинский исследовательский центр кардиологии» Министерства здравоохранения Российской Федерации (далее - Учреждение) в отношении обработки персональных данных в Учреждении.

## ВВЕДЕНИЕ

Настоящий документ предназначен для ознакомления неограниченного круга лиц.

Положение разработано в соответствии с действующим законодательством Российской Федерации о персональных данных (ПД):

- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»,

- Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации»,

- постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

- постановления Правительства Российской Федерации от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

- приказом ФСТЭК России от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Действие настоящей Политики распространяется на любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ) обезличивание, блокирование, удаление, уничтожение ПД.

Настоящее Положение подлежит пересмотру и, при необходимости, актуализации в случае изменений в законодательстве Российской Федерации о ПД.

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Персональные данные (ПД)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, паспортные данные, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация,

определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и здравоохранения.

**Обработка персональных данных** - действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке и действия (операции) совершаемые с персональными данными.

**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.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые работниками Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**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.

**Защита персональных данных** – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.

**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее положение имеет целью обеспечение обработки ПД в соответствии с требованиями действующего законодательства в сфере защиты ПД, обеспечение безопасности ПД, обрабатываемых в Учреждении, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПД.

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

При обработке ПД Учреждение придерживается следующих принципов:

- соблюдение законности получения, обработки, хранения, а так же других действий с ПД;

- обработка ПД исключительно в целях, перечисленных в статье 3 настоящего Положения;

- хранение ПД, обработка которых осуществляется с несвязанными между собой целями, в различных базах данных;

- содержание и объем обрабатываемых ПД соответствует заявленным целям обработки. Обрабатываемые ПД не являются избыточными по отношению к заявленным целям обработки;

- выполнение мер по обеспечению безопасности ПД, их точности, достаточности и других характеристик при обработке и хранении;

- соблюдение прав субъекта ПД на доступ к его ПД;

- соблюдение требований по уничтожению либо обезличиванию ПД по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Учреждение не производит обработку ПД субъектов ПД в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.

В Учреждении принятие решений на основании исключительно автоматизированной обработки ПД не производится.

## 2. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Информационные системы ПД, принадлежащие Учреждению, предназначены для обработки ПД:

- физических лиц, состоящих в трудовых отношениях с Учреждением, в том числе бывших сотрудников по срочному/ бессрочному трудовому или гражданско-правовому договору;

- физических лиц, обратившихся за медицинской помощью в Учреждение в рамках программы обязательного медицинского страхования;

- физических лиц, которым оказываются платные медицинские услуги;

- физических лиц, проходящих обучение в Учреждении.

## 3. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки ПД в Учреждении определены в соответствии с действующим законодательством и Уставом Учреждения. Основными целями обработки ПД являются:

- соблюдение законности получения, обработки, хранения, а так же других действий с ПД в рамках действующего законодательства;

- исполнение обязанностей работодателя в соответствии с законодательством Российской Федерации: ведение кадрового делопроизводства, обеспечение безопасности данных работника, организация командирования работников;

- исполнение гражданско-правовых договоров, стороной которого либо выгодоприобретателем по которому является субъект персональных данных;

- оказание медицинской помощи населению;

- осуществление учета и контроля в системе обязательного социального страхования,

- оказание образовательных услуг,

- архивное хранение документов в соответствии с законодательством Российской Федерации, в том числе выдача архивных справок по требованию субъекта персональных данных или его законного представителя.

## 4. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПЕРЕДАЧА ТРЕТЬИМ ЛИЦАМ

### 4.1. Обработка персональных данных.

Обработка ПД в Учреждении происходит как неавтоматизированным, так и автоматизированным способом.

К обработке ПД в Учреждении допускаются только работники, прошедшие определенную процедуру допуска, к которой относятся:

- ознакомление работника под роспись с локальными нормативными актами Учреждения, регламентирующими порядок и процедуру работы с ПД;

- взятие с работника подписки о соблюдении конфиденциальности в отношении ПД при работе с ними;

- получение работником и использование в работе индивидуальных атрибутов доступа к информационным системам Учреждения, содержащим в себе ПД. При этом каждому работнику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в информационные системы ПД.

Сотрудники, имеющие доступ к ПД, получают только те ПД, которые необходимы им для выполнения трудовых обязанностей по своей должности.

### 4.2. Хранение персональных данных.

ПД хранятся в бумажном и электронном виде.

В бумажном виде ПД должны храниться в специально оборудованных металлических шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов при этом находятся у ответственного сотрудника, назначаемого приказом по Учреждению.

В электронном виде ПД хранятся в базах данных информационных систем Учреждения, а также в архивных копиях баз данных.

Места хранения ПД, порядок хранения, учета и уничтожения к ним регламентируются внутренними документами Учреждения, утверждаемыми генеральным директором.

При хранении ПД соблюдаются организационные и технические меры по обеспечению их сохранности и исключению несанкционированного доступа к ним, в частности:

- назначение сотрудника, ответственного за обработку ПД в подразделении;

- ограничение физического доступа к местам обработки ПД;

- съемные электронные носители, на которых хранятся резервные копии ПД субъектов ПД, должны быть промаркированы и учтены в журнале регистрации, учета и выдачи внешних носителей для хранения резервных копий ПД;

- учет всех информационных систем и электронных и бумажных носителей, а также архивных копий;

- применение сертифицированных средств защиты информации и средств криптографической защиты информации.

**4.3. Передача персональных данных.**

Для целей обработки данных Учреждение может передавать ПД исключительно своим работникам и третьим лицам, подписавшим обязательство по обеспечению конфиденциальности и безопасности полученных сведений.

Также с письменного согласия пациента или его законного представителя допускается передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, использования в учебном процессе и в иных целях.

Предоставление сведений, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается:

- в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 Федерального закона Российской Федерации от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

- в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона Российской Федерации от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона Российской Федерации от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», для информирования одного из его родителей или иного законного представителя;

- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

- в целях расследования несчастного случая на производстве и профессионального заболевания;

- при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований регуляторов по защите персональных данных;

- в целях осуществления учета и контроля в системе обязательного социального страхования;

- в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

Передача ПД третьим лицам в остальных случаях возможна только с согласия субъекта ПД и только с целью исполнения обязанностей перед субъектом ПД в рамках договора, либо когда такая обязанность у Учреждения наступает в результате изменения требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В последнем случае Учреждение ограничивает передачу ПД запрошенным объемом. Передача данных, в данном случае, должна фиксироваться в соответствующем журнале ответственным лицом.

Передача ПД третьим лицам возможна только в рамках соглашения об информационном обмене или поручения оператора на обработку ПД. Исключением являются случаи предоставления информации в соответствии с требованиями о предоставлении информации, предъявленными уполномоченными государственными органами в соответствии с действующим законодательством.

В случае заключения поручения на обработку ПД с третьими лицами, в таком поручение должны быть определены перечень действий (операций) с ПД, которые будут совершаться лицом, осуществляющим обработку ПД, цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПД и обеспечивать безопасность ПД при их обработке, а также должны быть указаны требования к защите обрабатываемых ПД в соответствии со статьей 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

При передаче персональных данных в электронном виде третьим лицам по открытым каналам связи Учреждение обязано принимать все необходимые меры по защите передаваемой информации в соответствии с требованиями нормативно-методической документации регуляторов.

## 5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При обработке ПД Учреждение применяет необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, использования, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД.

5.2. Обеспечение безопасности ПД в Учреждении достигается следующими мерами:

- определение угроз безопасности ПД при их обработке в информационных системах ПД;

- применение организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПД;

- применение прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации средств защиты информации для нейтрализации актуальных угроз безопасности;

- оценка эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационной системы ПД;

- учет машинных носителей ПД;

- обнаружение фактов несанкционированного доступа к ПД и принятие мер по их нейтрализации;

восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- определение правил доступа к ПД, обрабатываемым в информационных системах ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД в информационных системах Учреждения;

- назначение сотрудника, ответственного за организацию обработки ПД;

- назначение структурного подразделения, ответственного за обеспечение безопасности ПД;

- назначение ответственных лиц по защите информационных систем Учреждения, содержащих ПД (администратор информационной системы, администратор безопасности, ответственный пользователь криптосредств);

- определение списка лиц, допущенных к работе с ПД;

- разработка и утверждение локальных нормативных актов Учреждения, регламентирующих порядок обработки ПД;

- проведение обучения и повышением осведомленности сотрудников в области защиты ПД;

- контроль соответствия обработки ПД Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПД, локальным актам Учреждения, в том числе контроль за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности информационных систем Учреждения;

- применение мер ответственности к должностным лицам Учреждения за нарушение установленных правил обработки ПД.

## 6. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его ПД, за исключением случаев, когда право субъекта ПД на доступ к его ПД может быть ограничено в соответствии с действующим законодательством.

6.2. Субъект ПД имеет право на получение следующей информации, касающейся обработки его ПД:

- подтверждение факта обработки ПД;

- правовые основания и цели обработки ПД;

- цели и применяемые способы обработки ПД;

- сведения о лицах (за исключением работников Учреждения), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора или на основании действующего законодательства;

- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения;

- сроки обработки ПД, в том числе сроки их хранения;

- порядок осуществления субъектом ПД своих прав;

- информацию об осуществленной или предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

Получить данную информацию субъект ПД может, обратившись с письменным запросом в Учреждение. Ответ, содержащий запрашиваемую информацию, либо мотивированный отказ в ее предоставлении направляется по адресу, указанному в запросе, в течение 30 дней.

6.3. Потребовать от Учреждения уточнения его ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.4. Отозвать согласие на обработку ПД в предусмотренных законом случаях.

## 7. ОБЯЗАННОСТИ УЧРЕЖДЕНИЯ

7.1. Учреждение обязуется осуществлять обработку ПД только с согласия субъектов ПД, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

7.2. При сборе ПД Учреждение обязуется по запросу субъекта ПД предоставлять информацию, касающуюся обработки его ПД, перечисленную в статье 6 настоящего Положения. В случае если предоставление ПД является обязательным в соответствии с действующим законодательством, Учреждение обязуется разъяснять субъекту ПД юридические последствия отказа предоставления ПД.

7.3. Если ПД получены не от субъекта ПД, Учреждение до начала обработки таких ПД обязуется предоставить субъекту ПД сведения, касающиеся обработки его ПД в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». В случаях, если Учреждение не является оператором ПД, полученных от субъектов ПД, обязанность по предоставлению субъекту ПД соответствующих сведений возлагается на оператора ПД, от которого эти данные получены.

7.4. Учреждение при обработке ПД обязуется принимать необходимые правовые, организационные и технические меры или обеспечить их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД. Описание принимаемых мер приведено в статье 5 настоящего Положения.

7.5. Учреждение обязуется отвечать на запросы субъектов ПД, их представителей, а также уполномоченного органа по защите прав субъектов ПД касательно обрабатываемых ПД в соответствии с требованиями действующего законодательства.

7.6. В случае предоставления субъектом ПД либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки ПД, Учреждение обязуется устранить данные нарушения в течение 7 (семи) рабочих дней и уведомить субъекта ПД о внесенных изменениях и предпринятых мерах.

7.7. В случае достижения целей обработки ПД Учреждение обязуется прекратить обработку ПД и уничтожить ПД в течение 30 (тридцати) календарных дней, если иное не предусмотрено условиями согласия субъекта ПД на обработку его ПД, договора или соглашения, заключенного с субъектом ПД.

7.8. Учреждение обязуется уведомлять уполномоченный орган по защите прав субъектов ПД о своем намерении осуществлять обработку ПД, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных». В случае изменения предоставленных сведений Учреждение обязуется предоставлять актуализированные сведения в течение 10 (десяти) рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПД.

* * * * *