Приложение №14
к приказу ФГБУ «НПЦ ЛМ
им. О.К. Скобелкина»
ФМБА России
от 27.07.2022 № 58

# ПОЛИТИКА

## в области обработки и защиты персональных данных в ФГБУ «НПЦ ЛМ им. О.К. Скобелкина» ФМБА России

### 1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее Политика) составлена в соответствии с п.2 ст.18.1 Федерального закона №152-ФЗ от 27.07.2006 года «О персональных данных» и является основополагающим внутренним регулирующим документом ФГБУ «НПЦ ЛМ им. О.К. Скобелкина» (далее - Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПД), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты персональных данных, необходимых для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, направлена на обеспечение защиты прав и свобод человека и гражданина при обработке ПД в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и соблюдение врачебной тайны.

1.3. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до ее утверждения.

1.4. Обработка ПД в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21.11.2011г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от27.07.206г. №152-ФЗ «О персональных данных» (далее – Федеральный закон о персональных данных);
- Постановлением Правительства от15.09.2018г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Иными нормативными правовыми актами РФ.

Кроме того, обработка ПД в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 ТК РФ), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация 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 ее размещения на сайте, если

иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения организации по адресу: 121165 Москва, ул. Студенческая, дом 40.

Электронная версия Политики размещена на официальном сайте учреждения: www.goslasmed.ru

## 2. Термины и принятые сокращения

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

**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;

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

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

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

**Блокирование персональных данных -** временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

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

**Автоматизированная обработка персональных данных -** обработка персональных данных с помощью средств вычислительной техники;

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Пациент -** физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания или состояния;

**Медицинская деятельность -** профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий;

**Лечащий врач -** врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

## 3. Принципы обеспечения безопасности персональных данных

**3.1.** Основной задачей обеспечения безопасности ПД при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПД, разрушения (уничтожения) или искажения их в процессе обработки.

**3.2.** Для обеспечения безопасности ПД Организация руководствуется следующими принципами:

- законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;
- системность: обработка ПД в Организации осуществляется с учетом всех взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;
- комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД.
- минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПД;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный отбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

**3.3.** В Организации не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатываемые Организацией ПД уничтожаются или обезличиваются.

**3.4.** При обработке ПД обеспечивается их точность, достаточность, а при необходимости и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПД.

## 4. Обработка персональных данных

**4.1. Получение ПД.**

4.4.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.4.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПД, перечне действий с ПД, сроке, в течении которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.4.3. Документы, содержащие ПД создаются путем:

- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, СНИЛС и др.);
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта к ПД к его ПД обрабатываемых Организацией, определяется в соответствии с действующим законодательством и внутренними нормативно-регулирующими документами Организации.

**4.2. Обработка ПД**

4.2.1. Обработка ПД осуществляется:

с согласия субъекта персональных данных либо при наличии иных оснований, предусмотренных пунктами 2-11 части 1 статьи 6 Федерального закона о персональных данных;

- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством РФ функций, полномочий и обязанностей;
- в случаях, когда обработка ПД необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее ПД, сделанные общедоступными субъектом персональных данных).
- Согласно пункту 6 части 1 статьи 6 Федерального закона обработка персональных данных, необходимая для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

Обработка специальных категорий персональных данных без получения согласия пациента для медицинской организации возможна в следующих случаях:

- обработка персональных данных для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну (пункт 4 части 2 статьи 10 Федерального закона о персональных данных).

Доступ Работников к обрабатываемым ПД осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Допущенные к обработке персональных данных Работники под роспись знакомятся с

документами Организации, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПД.

**4.2.2. Цели обработки ПД:**

- Обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», от29.11.2010г. №326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Постановлением Правительства Российской Федерации от 04.10.2012г. №1006 «Правила предоставления медицинскими организациями платных медицинских услуг».
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

**4.2.3. Категории субъектов персональных данных**

В организации обрабатываются ПД следующих субъектов:
- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся претендентами на рабочее место;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

**4.2.4. Персональные данные, обрабатываемые организацией:**

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в организацию;
- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании за медицинской помощью.

Полный список ПД представлен в Положениях об обработке ПД работников и пациентов, утвержденных директором Организации.

**4.2.5. Обработка персональных данных**

Обработка персональных данных ведётся:
- с использованием средств автоматизации;
- без использования средств автоматизации;

Обработка персональных данных должна осуществляться на основе принципов:
- Законности целей и способов обработки персональных данных и добросовестности;
- Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- Соответствия объёма и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных.

Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных.

**4.3. Хранение персональных данных**

4.3.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

4.3.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемом помещении с ограниченным правом доступа (регистратура, кабинет отдела кадров, кабинет статистики), в запираемых шкафах.

4.3.3. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

### 4.4. Уничтожение ПД

4.4.1. Уничтожение документов (носителей), содержащих ПД производится путём сожжения, дробления (измельчения), превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

### 4.5. Передача ПД

4.5.1. Организация передает ПД третьим лицам в следующих случаях:

- субъект выразил своё согласие на такие действия;
- передача предусмотрена Российским законодательством в рамках установленной законодательной процедуры.

4.5.2. Перечень третьих лиц, которым передаются ПД:

- Пенсионный фонд РФ (на законных основаниях);
- налоговые органы РФ (на законных основаниях);
- Фонд социального страхования - ФСС (на законных основаниях);
- банки для начисления заработной платы (на основании трудового договора либо договора подряда);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- юридические фирмы, банки, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта);

## 5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных программно-аппаратных средств, обеспечивающих защиту ПД.

5.5. Основными мерами защиты ПД, используемыми Организацией являются:

5.5.1. Назначение лица ответственного за обработку ПД, которое осуществляет

организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД;

5.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;

5.5.3. Разработка политики в отношении обработки ПД.

5.5.4. Установление прав доступа к ПД, обрабатываемым в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПД в ИСПД.

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

5.5.6. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности.

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.5.8. Межсетевой экран и средство обнаружения вторжения.

5.5.9. Соблюдение условий, обеспечивающих сохранность ПД и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых мер по обеспечению безопасности ПД.

5.5.11 Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.13. Обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям Законодательства РФ о персональных данных, в том числе, требованиям к защите ПД, документам, определяющим политику Организации в отношении обработки ПД, локальным актам по вопросам обработки ПД.

5.5.14. Осуществление внутреннего контроля и аудита.

## 6. Основные права субъекта ПД и обязанности Организации

### 6.1. Основные права субъекта ПД.

Субъект ПД имеет право на получение информации, касающейся обработки его ПД, в том числе содержащей:

- подтверждение факта обработки ПД оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора) , которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с оператором или на основании Федерального Закона;
- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки ПД, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных Федеральным законом о персональных данных;
- информацию об осуществлённой или предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;
-иные сведения, предусмотренные Федеральным законом о персональных данных или другими федеральными законами.

Субъект ПД вправе требовать от оператора 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, а также принимать предусмотренные законом меры по защите своих прав.

**6.2. Обязанности Организации**.

Организация обязана:

- при сборе ПД предоставить информацию об обработке ПД субъекту ПД;
- в случаях если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.

## 7. Опубликование сведений о медицинской деятельности и о медицинских работниках

Согласно пункту 7 части 1 статьи 79 Федерального закона от 21.11.2011г. №323-ФЗ «Об основах охраны здоровья граждан в РФ» медицинская организация обязана информировать граждан в доступной форме, в том числе с использованием сети «Интернет», об осуществляемой медицинской деятельности и о медицинских работниках медицинских организаций, об уровне их образования и об их квалификации, а также предоставлять иную необходимую информацию для проведения независимой оценки качества оказания услуг медицинскими организациями информацию.

Во исключение данной правовой нормы приказом Минздрава России от 30.12.2014 №956н утверждены требования к содержанию и форме предоставления информации о деятельности медицинских организаций, размещаемой на официальных сайтах Министерства здравоохранения Российской Федерации, органов государственной власти субъектов Российской федерации, органов местного самоуправления и медицинских организаций в информационно-телекоммуникационной сети "Интернет". Обработка персональных данных лиц, не предусмотренных данным правовым актом, а также обработка категорий персональных данных в объеме, превышающем объем определенный приказом, возможен только с согласия субъекта персональных данных.

## 8. Контактная информация

**Наименование оператора**: Федеральное государственное бюджетное учреждение «Научно-практический центр лазерной медицины имени О.К.Скобелкина» Федерального медико–биологического агентства

**Адрес местонахождения оператора**: 121165 Москва, ул. Студенческая, дом 40

**Телефон, e-mail**: 8 (495) 661-01-32, gnc_lazmed@fmbamail.ru.

**Официальный сайт**: https://www.goslasmed.ru/

**Ответственным за организацию обработки персональных данных**:

Заместитель директора по медицинской части Штанев Е.И.