Санкт-петербургское государственное учреждение здравоохранения
«Городской врачебно-физкультурный диспансер»

П Р И К А З

15 декабря 2025 г. **№ 117**

Об утверждении документов,
регламентирующих обработку
персональных данных
в СПб ГБУЗ ГВФД

В целях исполнения требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21, других нормативных актов РФ и обеспечения защиты персональных данных и иной конфиденциальной информации

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке и защите персональных данных пациентов СПб ГБУЗ ГВФД согласно Приложению к настоящему Приказу.
2. Ответственному за защиту информации, содержащей персональные данные на объектах информатизации СПб ГБУЗ ГВФД, специалиста по защите информации – Леонгардт Александра Альбертовича руководствоваться в работе выше утвержденным Положением согласно Приложению к настоящему Приказу.
3. Системному администратору Павлову Ивану Геннадьевичу опубликовать выше утвержденное Положение согласно Приложению к настоящему Приказу на официальном сайте СПб ГБУЗ ГВФД в информационно-телекоммуникационной сети «Интернет» в течение 5 (пяти) рабочих дней со дня подписания настоящего Приказа.
4. Секретарю Наумовой Е.А. ознакомить вышеуказанных ответственных лиц с настоящим приказом под подпись.
5. Контроль за исполнением приказа возложить на начальником АПО Кокорина И.С.

Главный врач СПб ГБУЗ ГВФД **А.В. Калинин**

Приложение к Приказу
СПб ГБУЗ ГВФД
От 15.12.2025 № 117

Положение
об обработке и защите персональных данных пациентов Санкт-Петербургского государственного бюджетного учреждения здравоохранения «Городской врачебно-физкультурный диспансер»

1. Общие положения

1.1 Настоящее Положение об обработке и защите персональных данных пациентов Санкт-Петербургского государственного бюджетного учреждения здравоохранения «Городской врачебно-физкультурный диспансер» (далее – Положение) определяет цели, принципы, порядок и условия любых действий (операций) или совокупности 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 (далее – Обработка персональных данных) с персональными данными пациентов Санкт-Петербургского государственного бюджетного учреждения здравоохранения «Городской врачебно-физкультурный диспансер» (далее – Диспансер), устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, связанных с обработкой и защитой персональных данных.

Все вопросы, связанные с обработкой и защитой персональных данных, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации в области персональных данных.

1.2. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных», Федеральным законом от 21.11.2011 № 323 «Об основах охраны здоровья граждан в Российской Федерации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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» и иными действующими нормативными правовыми актами Российской Федерации.

1.3. Цель обработки персональных данных — оказание услуг, выполнение работ для обеспечения реализации предусмотренных законодательством Российской Федерации полномочий органов государственной власти Санкт-Петербурга в сфере здравоохранения по охране здоровья граждан, занимающихся физической культурой и спортом.

1.4. Положение утверждается приказом главного врача. Все изменения и дополнения в Положение вносятся в том же порядке.

2. Принципы обработки и защиты персональных данных

2.1. Обработка организована Диспансером на принципах, предусмотренных Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных» и настоящим Положением.

2.2. Обработка персональных данных организована Диспансером на принципах:

2.2.1. законности целей и способов обработки персональных данных, добросовестности и справедливости в деятельности Диспансера;

2.2.2. ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;

2.2.3. достоверности персональных данных, их достаточности для целей обработки;

2.2.4. обработки только персональных данных, которые отвечают целям их обработки. Недопустима обработка персональных данных, несовместимая с целями сбора персональных данных;

2.2.5. соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

2.2.6. недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

2.2.7. обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

2.2.8. хранения персональных данных 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.

2.3. Персональные данные обрабатывают с использованием средств автоматизации или без них.

3. Порядок обработки персональных данных пациента

1. В соответствии с целью, указанной в п. 1.3 Положения, в Диспансере обрабатываются следующие персональные данные:

- фамилия, имя, отчество (последнее - при наличии);
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном

(персонифицированном) учете в системе обязательного пенсионного страхования;

- анамнез;
- диагноз;
- вид оказанной медицинской помощи;
- объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
- результат обращения за медицинской помощью;
- сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты;
- Контактные телефоны;
- Почтовый и электронный адреса;
- Вид спорта;
- Этап спортивной подготовки;
- И иную информацию, если это обеспечено требованиями законодательства РФ и иных подзаконных актов.

3.2. Диспансер не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством Российской Федерации и уставной деятельности диспансера.

3.3. Действие настоящего Положения не распространяется на отношения, возникающие:

3.3.1. при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных фондов в соответствии с законодательством об архивном деле в Российской Федерации;

3.2.2. при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

3.3. Безопасность персональных данных, обрабатываемых Диспансером, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.

3. Обработка персональных данных пациента

4.1. Обработка персональных данных осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, обезличивания, блокирования, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

4.2. Обработка персональных данных в Диспансере выполняется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

4.3. Обработка персональных данных осуществляется:

4.3.1. С согласия пациента или его законного представителя на обработку персональных данных пациента, если иное не предусмотрено законодательством в области персональных данных. Согласие предоставляется пациентом или его законным представителем лично либо в форме электронного документа, подписанного электронной подписью.

4.3.2. Обработка биометрических персональных данных допускается только при наличии письменного согласия пациента или его законного представителя. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 Федерального закона 27.07.2006 № 152 «О персональных данных».
4.4. В Диспансере для обработки персональных данных используются следующие информационные системы:

- Медицинская информация система;
- Лабораторная информационная система;
- Локальная система хранения и передачи данных.

4.5. Передача (распространение, предоставление, доступ) персональных данных пациентов осуществляется Диспансером в случаях и в порядке, предусмотренных законодательством в области персональных данных и настоящего Положения.

5. Хранение персональных данных

5.1. Персональные данные пациентов могут быть получены, проходить дальнейшую обработку и передаваться на хранение в электронном виде, а так же на бумажных носителях.
5.2. Хранение персональных данных в форме, позволяющей определить пациента, 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. Исключение – случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого является пациент.
5.3. Персональные данные на бумажных носителях хранятся в Диспансере в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 № 125 «Об архивном деле в Российской Федерации», перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения, утв. приказом Росархива от 20.12.2019 № 236).
5.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.
5.5. Персональные данные зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.
5.6. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых информационных ресурсах.

6. Прекращение обработки персональных данных

6.1. Обработка персональных данных в Диспансере прекращается в следующих случаях:
6.1.1. при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки – в течение трех рабочих дней с даты выявления такого факта;
6.1.2. при достижении целей обработки персональных данных;
6.1.3. истечении срока действия или при отзыве субъектом ПДн согласия на обработку его персональных данных, если в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ их обработка допускается только с согласия;
6.1.4. при обращении субъекта персональных данных к Диспансеру с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ). Срок прекращения обработки – не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

7. Блокирование и уничтожение персональных данных

7.1. Диспансер блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

7.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональных данных уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

7.3. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления пациентом (его законным представителем) подтверждающих сведений.

7.4. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

7.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является пациент или его законный представитель, иным соглашением между ним и Диспансером, либо если Диспансер не вправе обрабатывать персональные данные без согласия пациента или его законного представителя на основаниях, предусмотренных федеральными законами.

7.6. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

7.7. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва пациентом или его законным представителем согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является пациент или его законный представитель, иное соглашение между ним и Диспансером. Кроме того, персональные данные уничтожаются в указанный срок, если Диспансер не вправе обрабатывать их без согласия пациента или его законного представителя на основаниях, предусмотренных федеральными законами.

7.8. Отбор материальных носителей (документы, жесткие диски, твёрдотельные накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляет специалист по защите информации (в составе комиссии).

7.9. Уничтожение персональных данных осуществляет специалист по защите информации (в составе комиссии).

7.9.1. специалист по защите информации (в составе комиссии) составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

7.9.2. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

Персональные данные на физических электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

7.9.3. Специалист по защите информации (в составе комиссии) подтверждает уничтожение персональных данных согласно Требованиям к подтверждению

уничтожения персональных данных, утвержденным приказом Роскомнадзора от 28.10.2022 № 179, а именно:
7.9.3.1. актом об уничтожении персональных данных – если данные обрабатываются без использования средств автоматизации;
7.9.3.2. актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных – если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.
Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.
Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом главного врача Диспансера.
7.9.4. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных, акт передается на хранение ответственному лицу.
7.9.5. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

8. Передача персональных данных

8.1. Диспансер передает персональные данные третьим лицам, если пациент выразил свое согласие на такие действия или передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.
8.2. Перечень третьих лиц, которым передаются персональных данных: в соответствии с законодательством РФ для осуществления своей основной деятельности, а так же предоставления информации органам, имеющим право на получение такой информации в соответствии законными правами.
8.3. Диспансер не осуществляет трансграничную передачу персональных данных.

9. Доступ к персональным данным

9.1. Порядок доступа пациента к его персональным данным, обрабатываемым Диспансером, определяется в соответствии с законодательством РФ.
9.2. Доступ Работников Диспансера к обрабатываемым персональным данным пациента осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Диспансера.
9.3. Допущенные к обработке персональных данных Работники под подпись знакомятся с документами организации, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных Работников.

10. Защита персональных данных

10.1. Основными мерами защиты персональных данных, используемыми Диспансером, являются:
10.1.1. Назначение лица ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Организацией и ее работниками требований к защите персональных данных.
10.1.2. Определение актуальных угроз безопасности персональных данных при их обработке в ИСПДн и разработка мер и мероприятий по защите персональных данных.
10.13. Разработка Положения в отношении обработки персональных данных пациентов.
10.1.4. Установление правил доступа к персональных данных, обрабатываемым в ИСПДн, а также обеспечения регистрации и учета всех действий, совершаемых с персональных данных в ИСПДн.

10.1.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их должностными обязанностями.
10.1.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей персональных данных, обеспечение их сохранности.
10.1.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
10.1.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.
10.1.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.
10.1.10. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных.
10.1.11. Установление правил доступа к обрабатываемым персональных данных, обеспечение регистрации и учета действий, совершаемых с персональных данных, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.
10.1.12. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
10.1.13. Обучение работников Диспансера, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Диспансера в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.
10.1.14. Осуществление внутреннего контроля и аудита.
10.1.15. Работники Диспансера, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящим Положением и изменениями к нему, локальными актами по вопросам обработки персональных данных.

11. Права пациента

11.1. Пациент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Диспансером;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения Диспансера, сведения о лицах (за исключением работников Диспансера), которые имеют доступ к персональным данным, или которым могут быть раскрыты персональные данные на основании договора с Диспансером или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их 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 Федеральным законом от 27.07.2006 № 152-ФЗ;
- 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 Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами.

11.2. Пациент вправе требовать от Диспансера уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

11.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

12. Обязанности Диспансера

12.1. Диспансер обязан:

- при сборе персональных данных предоставить информацию пациенту или его законному представителю об обработке персональных данных пациента;
- при отказе в предоставлении персональных данных субъекту разъясняются последствия такого отказа;
- опубликовать в открытом источнике или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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 ;
- давать ответы на запросы и обращения пациентов или их законных представителей, и уполномоченного органа по защите прав пациентов в соответствии с действующим законодательством РФ;
- не сообщать персональные данные пациента третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством РФ;
- не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они предоставлены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- разрешать доступ к персональным данным пациента только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций.

13. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

13.1 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством.

13.2 Лица организации, получившие в установленном порядке доступ к персональным данным пациента, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента привлекаются Оператором к дисциплинарной ответственности в порядке предусмотренной действующих законодательством Российской Федерации.