

к приказу от « 13 » апреля 2023 г. № 48



УТВЕРЖДАЮ

Директор

ЛПУ «Железноводская
бальнеогрязелечебница»

А.М. Шатров

2023 г.

ПОЛОЖЕНИЕ

о порядке обработки персональных данных отдыхающих в Лечебно-профилактическом учреждении «Железноводская бальнеогрязелечебница»

1. Общие положения

1.1. Настоящее Положение о порядке обработки персональных данных (далее – Положение) в Лечебно-профилактическом учреждении «Железноводская бальнеогрязелечебница» (далее – Учреждение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Федеральным законом РФ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации (в ред. от 24.07.2023 N 386-ФЗ)», «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства РФ № 1119 от 01.11.2012 г., иными нормативными актами Российской Федерации.

1.2 Основными целями настоящего Положения являются:

- определение порядка обработки персональных данных субъектов Учреждения;
- обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну;
- установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.

Все изменения в Положение вносятся приказом директора.

1.4 Сотрудники, допущенные к работе с персональными данными отдыхающих, в обязательном порядке под роспись знакомятся с настоящим Положением. Субъекты персональных данных, обрабатываемых Учреждением, имеют право знакомиться с настоящим Положением в части, касающейся обработки персональных данных в соответствии со статьей 14 Федерального закона «О персональных данных».

2. Основные понятия и состав персональных данных

2.1 Для целей настоящего Положения используются следующие основные понятия:

- персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, информация о состоянии здоровья, другая информация;

- 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, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- конфиденциальность персональных данных – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

- распространение персональных данных – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

- предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- доступ к информации - возможность получения информации и ее использования;

- 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;

- информация – сведения (сообщения, данные) независимо от формы их представления;

- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2.2. В Учреждении обрабатываются следующие документы, содержащие персональные данные отдыхающих:

— комплексы документов, сопровождающие процесс оформления отдыхающего для проживания в санатории;

— результаты медицинского обследования;

— подлинники и копии отчетных, аналитических и справочных материалов, передаваемых Руководителю Учреждения, копии отчетов, направляемых в органы статистики, вышестоящие органы управления и другие учреждения (обезличенные данные);

— иные документы.

2.3 Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

3. Основные принципы обработки персональных данных субъекта персональных данных

3.1. Обработка персональных данных осуществляется на основе следующих 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 Учреждения;

- соответствия объема 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;

- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи Учреждению своих персональных данных.

3.4. Учреждение распоряжается персональными данными в пределах, установленных законодательством Российской Федерации и настоящим Положением.

3.5. Обработка персональных данных осуществляется исключительно в целях предоставления санаторно-курортных услуг, организации лечебного процесса, проживания, обеспечения соблюдения законов и иных нормативных правовых актов, контроля количества и качества выполняемой работы, обеспечения сохранности имущества Учреждения.

3.6. Учреждение в ходе своей деятельности может предоставлять и (или) поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. При этом обязательным условием предоставления и (или) поручения обработки персональных данных другому лицу является обязательство сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке.

3.7. При принятии решений, затрагивающих интересы субъекта, Учреждение не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.8. Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается Учреждением за счет собственных средств в порядке, установленном законодательством Российской Федерации.

3.9 При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

3.10. Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

- Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным 5 февраля 2010 г.
- специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282
- внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

3.11. Защита персональных данных отдыхающих возлагается по соответствующим направлениям на:

- главную медицинскую сестру;
- главного специалиста отдела продаж;
- главного экономиста;
- главного бухгалтера;
- заведующих медицинскими отделениями.

3.12. Работа с обращениями субъектов персональных данных проводится на основании «Регламента обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных».

4. Обработка персональных данных

4.1 Персональные данные отдыхающих обрабатываются в следующих структурных подразделениях Учреждения:

- отдел продаж;
- бухгалтерия;
- медицинские отделения.

4.2. При необходимости допускается обработка персональных данных в других структурных подразделениях Учреждения при условии их обработки специально уполномоченными лицами и с соблюдением требований настоящего Положения.

4.3 Доступ к персональным данным отдыхающих имеют:

- директор;
- главный бухгалтер;
- заместитель главного бухгалтера;
- бухгалтер;
- бухгалтер-кассир;
- главный экономист;
- главная медицинская сестра;
- главный специалист отдела продаж;
- старший специалист отдела продаж;
- специалист отдела продаж;
- заведующие медицинскими отделениями;
- врачи всех специальностей;
- старшие медицинские сестры отделений;
- медицинские сестры отделений.

4.4 При оформлении в санаторий отдыхающий представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- санаторно-курортную карту;
- в отдельных случаях с учетом специфики обследования в Учреждении действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

4.4.1. Администратор вносит персональные данные клиента в базу данных ПО «ОТЕЛЬ».

4.4.2. Все персональные данные субъекта получаются у него самого. При этом должно быть получено письменное согласие отдыхающего на обработку его персональных данных (приложение № 1). Если персональные данные клиента возможно получить только у третьей стороны, то отдыхающий должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (приложение № 2). Учреждение должно сообщить отдыхающему о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа их предоставить.

4.5. Персональные данные хранятся:

- в электронном виде (на персональных компьютерах, а также на сменных магнитных, оптических и других цифровых носителях);
- на бумажных носителях, в том числе в медицинских картах, в специально оборудованных шкафах и сейфах. Медицинские карты прошедших обследование, лечение субъектов хранятся в архиве Учреждения.

4.6 Порядок обработки персональных данных с использованием средств автоматизации:

4.6.1 Обработка персональных данных отдыхающих в автоматизированных информационных системах персональных данных осуществляется с использованием специализированного программного обеспечения "ОТЕЛЬ".

4.6.2 Доступ лиц к обработке персональных данных в информационных системах персональных данных (далее – ИСПДн) осуществляется в соответствии с приказом руководителя Учреждения.

4.6.3 Работником, допущенным к персональным данным отдыхающих, подписывается Обязательство о неразглашении в установленном порядке.

4.6.4 При первичном допуске к работе в ИСПДн пользователь знакомится с требованиями нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, о чем делается запись в журнале ознакомления с организационно-распорядительной документацией, проходит инструктаж у ответственного за обеспечение безопасности ПДн и администратора безопасности по вопросам организационного и технического характера, получает под роспись личный текущий логин и пароль.

4.6.5 В согласованное с ответственным за обеспечение безопасности персональных данных время пользователь принимает и включает ПЭВМ и необходимое периферийное оборудование, визуально убеждается в целостности печатей, исправности и нормальном функционировании ИСПДн.

4.6.6 Для входа на автоматизированное рабочее место пользователь должен использовать персональный идентификатор и пароль, зарегистрированные в ИСПДн.

4.6.7 Ввод персональных данных в ИСПДн осуществляется пользователями ИСПДн следующими способами:

- ввод информации с клавиатур рабочих станций, каждая из которых закреплена за конкретным сотрудником;
- путем копирования и (или) переноса ее с отчуждаемых носителей информации (Flash-накопители, FDD, CD, DVD-CD, внешние HDD), при этом в ИСПДн не допускается использование не учтенных машинных носителей информации.

Иные способы ввода информации, в том числе речевой, в ИСПДн запрещены.

4.6.8 После ввода информации в ИСПДн она подлежит хранению только в тех ресурсах, которые определены как защищаемые. К защищаемым ресурсам применяются правила разграничения доступа. Для уничтожения, копирования и (или) переноса информации пользователь должен обратиться к защищаемому ресурсу и после проверки его полномочий подсистемой разграничения доступа выполнить необходимые действия.

4.6.9 Для доступа к защищаемым ресурсам и документам пользователь использует штатное программное обеспечение ИСПДн.

4.6.10 При необходимости пользователь выводит информацию, содержащую персональные данные из ИСПДн следующим образом:

- на печатающие устройства, на предварительно учтенные бумажные носители;
- копированием персональных данных на учтенные машинные носители информации (ЖМД, ГМД, оптические диски, Flash-накопители).

Иные способы вывода информации, в том числе речевой, из ИСПДн запрещены.

4.7 Порядок обработки персональных данных без использования средств автоматизации:

4.7.1 При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.7.2 При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

4.7.3 Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

4.7.3.1 Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

4.7.3.2 К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

4.7.3.3 При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.7.4 Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах и сейфах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

4.7.5 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.7.6 Уничтожение персональных данных на материальных носителях производится комиссией, состоящей из сотрудников Учреждения, по акту согласно Порядку уничтожения материальных носителей персональных данных отдыхающих и работников ЛПУ «Железноводская бальнеогрязелечебница».

4.8 Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

4.9 Порядок работы в помещениях, в которых ведется обработка персональных данных.

4.9.1 Прием посетителей, отдыхающих в помещениях, в которых ведется обработка персональных данных, должен осуществляться только в те часы, которые ежедневно выделяются для этой цели. В другое время в помещении не должны находиться посторонние лица, в том числе сотрудники Учреждения. Приемные часы должны быть разными для сотрудников Учреждения и лиц, не входящих в эту категорию. Прием посетителей должен быть организован таким образом, чтобы в помещении не было лиц, ожидающих приема.

4.9.2 В часы приема посетителей, отдыхающих сотрудники, в том числе медицинские работники, не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На столе работника, ведущего прием, не должно быть никаких документов, кроме тех, которые касаются данного посетителя.

4.9.3 Ответы на вопросы даются только лично тому лицу, которого они касаются. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону. Ответы на письменные запросы других учреждений и организаций даются в письменной форме на бланке Учреждения и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

4.9.4 При выдаче медицинских заключений необходимо удостовериться в личности субъекта, которому выдается заключение. Не разрешается выдавать его родственникам или знакомым лица, которому выдается заключение.

4.9.5 Уборка помещений допускается только в присутствии сотрудников отдела. Мусор, выносимый из помещений, должен сжигаться.

4.9.6 Любые посторонние лица, в том числе сотрудники Учреждения,

функциональные обязанности которых не связаны с работой отдела, не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе.

4.9.7 Бумажные носители, содержащие ПДн (медицинские карты, договоры), дела, картотеки, учетные журналы, книги учета хранятся в рабочее и нерабочее время в надежно запирающихся шкафах. Работникам не разрешается при любом по продолжительности выходе из помещения оставлять какие-либо документы на рабочем столе или оставлять шкафы незапертыми.

4.9.8 На рабочем столе работника должен всегда находиться только тот массив документов и учетных карточек, с которым в настоящий момент он работает. Другие документы, дела, карточки, журналы должны находиться в запертом шкафу.

4.9.9 В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями должны быть убраны в запирающиеся шкафы.

4.9.10 Запрещается обработка персональных данных под диктовку.

4.9.11 Экран монитора в помещении необходимо располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

4.9.12 При любом по продолжительности выходе из помещения необходимо закрывать дверь на ключ.

5. Особенности передачи персональных данных третьим лицам

5.1 При передаче персональных данных отдыхающих должны соблюдаться следующие требования:

5.1.1 Не сообщать персональные данные отдыхающего третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных федеральными законами. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению Учреждения, отсутствует угроза жизни или здоровью субъекта, представитель Учреждения обязан отказать в предоставлении персональных данных лицу.

5.1.2 Персональные данные отдыхающих могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого отдыхающего.

5.1.3 Не сообщать персональные данные отдыхающего в коммерческих целях без его письменного согласия.

5.1.4 Предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

5.1.5 Разрешать доступ к персональным данным отдыхающих только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

5.1.6 Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных (Приложение 3) в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана.

6. Типовые формы

6.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма) согласно пункту 7 Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки

персональных данных, осуществляемой без использования средств автоматизации» должны удовлетворять следующим требованиям:

6.1.1 Типовые формы обрабатываются вместе со связанными с ней документами: инструкция по заполнению типовой формы, реестры и журналы.

6.1.2 Типовая форма или связанные с ней документы (карточки, реестры и журналы) должны содержать:

- сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;
- наименование и адрес учреждения;
- фамилию, имя, отчество и адрес субъекта персональных данных;
- источник получения данных;
- сроки их обработки;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- общее описание используемых учреждением способов обработки персональных данных.

6.1.3 Форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими данными, не нарушая прав и законных интересов иных субъектов персональных данных.

6.1.4 Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.1.5 Типовая форма заполняется в соответствии с Инструкцией по заполнению типовых форм, содержащих персональные данные отдыхающих (пациентов) в ЛПУ «Железноводская бальнеогрязелечебница» (приложение 4).

7. Права субъектов персональных данных

7.1 Субъекты персональных данных имеют право на:

7.1.1 свободный, бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных Федеральным законом;

7.1.2 полную информацию об их персональных данных и их обработке;

7.1.3 требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона «О персональных данных»;

7.1.4 требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта обо всех произведенных в них исключениях, исправлениях или дополнениях;

7.1.5 обжалование в суд любых неправомерных действий или бездействий при обработке и защите персональных данных.

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

8.1. Ответственность за утрату материальных носителей, содержащих персональные данные, или разглашение сведений, содержащихся в них, персонально несет каждый работник в соответствии с действующим законодательством Российской Федерации.

8.2. По факту утраты (разглашения) материальных носителей с персональными данными ставится в известность руководитель Учреждения, и его приказом назначается комиссия для проведения служебного расследования.

8.3. Комиссия устанавливает обстоятельства происшествия и виновных в утрате (разглашении), а также причины и условия, способствующие этому.

8.4. Служебное расследование проводится в срок не более одного месяца со дня обнаружения факта утраты (разглашения). Результаты расследования докладываются руководителю Учреждения, назначившему комиссию. На утраченные документы составляется акт, на основании которого делаются соответствующие отметки в учетных

формах.

8.5 По результатам расследования руководитель Учреждения принимает решение о привлечении виновных к дисциплинарной или иной (административной, уголовной) ответственности, предусмотренной действующим законодательством Российской Федерации.

СОГЛАСОВАНО: