УТВЕРЖДЕНА:
Генеральный директор – главный врач
АО «Санаторий «Чувашия»
_____Ю.Л.Симунов
Приказ № 70 от 28 июня 2017 года

Политика
Акционерного общества «Санаторий «Чувашия»
в отношении обработки персональных данных

(включая сведения о реализуемых требованиях
к защите персональных данных)

Назначение и область действия Политики

Настоящий документ (далее – Политика) является систематизированным изложением целей, принципов, способов и условий обработки персональных данных, сведений о реализуемых требованиях к порядку обработки и защите персональных данных в АО «Санаторий «Чувашия» (далее – Общество).

Политика определяет позицию и намерения Общества в области обработки и защиты персональных данных, соблюдения прав и свобод каждого человека и, в особенности, права на неприкосновенность частной жизни, личную и семейную тайну.

Политика основана на требованиях Федерального закона РФ «О персональных данных», иных нормативно-правовых актах РФ, устанавливающих порядок обработки и защиты персональных данных. Политика является публичным документом.

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» Общество является оператором персональных данных.

Определения

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). К такой информации, в частности, можно отнести: ФИО, год, месяц, дату и место рождения, адрес, данные документов, удостоверяющих личность, сведения о семейном, имущественном положении, сведения об образовании, профессии, доходах, а также другую информацию.

Под обработкой персональных данных понимается 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.

Субъекты персональных данных

Общество обрабатывает персональные данные следующих лиц:

- физических лиц, состоящих (состоявших) в трудовых отношениях с Обществом;
- физических лиц, состоящих (состоявших) в договорных и иных гражданско-правовых отношениях с Обществом;
- физических лиц, обратившихся в Общество с целью получения информации, заключения договора либо вступления в иные гражданско-правовые отношения с Обществом, связанные с оказанием санаторно-курортных и медицинских услуг;
- физических лиц, уполномоченные доверенностью Общества на представление интересов от имени Общества;
- физических лиц, документы которых получены Обществом от третьих лиц;
- акционеров и членов совета директоров Общества;
- иных физических лиц, чьи персональные данные обрабатываются Обществом в соответствии с требованиями законодательства;
- представителей вышеперечисленных физических лиц.

Цели обработки персональных данных

Обработка персональных данных граждан осуществляется Обществом в целях:

- обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов, в т.ч. Федерального закона № 152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), Устава и локальных нормативных актов Общества;
- учета персональных данных физических лиц;

- заключения трудовых договоров и соглашений с работниками;
- оказания медицинских услуг и защиты прав пациента (при установлении медицинского диагноза, определении методики лечения заболеваний, оформлении медицинской документации, оказании всех видов медицинских услуг),
- совершения гражданско-правовых сделок и исполнения иных гражданско-правовых обязательств, связанных с предоставлением гражданам санаторно-курортных услуг;
- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальными потребителями/клиентами с помощью средств связи;
- содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, страхования работников;
- обеспечения безопасности физических лиц и представителей юридических лиц, являющихся контрагентами Общества, обеспечение безопасности информации, обрабатываемой в помещениях Общества.

Принципы обработки персональных данных

- законная и справедливая основа обработки персональных данных, законные способы обработки персональных данных;
- ограничение обработки персональных данных достижением заранее определенных и законных целей, указанных в пункте «Цели обработки персональных данных»;
- недопущение объединения баз данных, содержащих персональных данных, обработка которых осуществляется в несовместимых между собой целях;
- обработка только тех персональных данных, которые отвечают целям обработки;
- соответствие содержания и объема обрабатываемых персональных данных целям обработки, недопустимость избыточности обрабатываемых персональных данных по отношению к заявленным целям обработки;
- обеспечение точности персональных данных, их достаточности и актуальности по отношению к целям обработки персональных данных;
- обеспечение принятия необходимых мер по удалению или уточнению неполных или неточных данных;
- осуществление 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.

Способы обработки персональных данных

– автоматизированный, неавтоматизированный, смешанный.

Условия обработки персональных данных

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении конституционных прав граждан Российской Федерации, Общество обеспечивает надежную защиту персональных данных.

Под безопасностью персональных данных Общество понимает защищенность 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 и принимает необходимые правовые, организационные и технические меры для защиты персональных данных.

Общество обрабатывает персональные данные с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных».

Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Обработка персональных данных без согласия субъекта персональных данных осуществляется только в случаях, предусмотренных законодательством РФ.

Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Общества определяются перечень действий (операций) с персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению Общества, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество. Лицо, осуществляющее обработку персональных данных по поручению Общества, несет ответственность перед Обществом.

В случаях, установленных законодательством Российской Федерации, в т.ч. с согласия гражданина, Общество вправе осуществлять передачу персональных данных граждан.

Права граждан в части обработки персональных данных

Гражданин, персональные данные которого обрабатываются Обществом, имеет право:

- получать от Общества:
  - подтверждение факта обработки персональных данных;
  - сведения о правовых основаниях и целях обработки персональных данных;
  - сведения о применяемых способах обработки персональных данных;
  - сведения о наименовании и месте нахождения Общества;
  - перечень обрабатываемых персональных данных, относящихся к гражданину, от которого поступил запрос и информацию об источнике их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
  - сведения о сроках обработки персональных данных, в том числе о сроках их хранения;
  - сведения о порядке осуществления гражданином прав, предусмотренных ФЗ «О персональных данных»;
  - информацию об осуществляемой или о предполагаемой трансграничной передаче персональных данных;
  - наименование и адрес лица, осуществляющего обработку персональных данных по поручению Общества;
  - иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами;
- требовать уточнения своих 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;

- отозвать свое согласие на обработку персональных данных. В случае отзыва гражданином своего согласия на обработку персональных данных Общество в случаях, определенных ФЗ «О персональных данных» (если обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей; обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве; обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно; обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных; обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных; осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе; осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.), вправе продолжить обработку персональных данных без согласия гражданина;

- требовать устранения неправомерных действий Общества в отношении его персональных данных;

- обжаловать действия или бездействие Общества в уполномоченный надзорный орган (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что Общество осуществляет обработку его персональных данных с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

Обязанности Общества

Общество при обработке персональных данных выполняет свои обязанности как оператора персональных данных, предусмотренные Федеральным законом «О персональных данных».

Общество принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Общество самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено федеральными законами.

Общество обеспечивает бесплатный неограниченный доступ к Политике, к сведениям о реализуемых требованиях к защите персональных данных путем размещения своем на официальном сайте Общества http://www.sanatory-chuvashia.com/ и в помещении, где осуществляется регистрация и размещение граждан (регистратура первого этажа).

Конфиденциальность

Общество и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

При обработке персональных данных Общество обязуется соблюдать требования, установленные законодательством к защите обрабатываемых персональных данных.

Общество и иные лица, получившие доступ к персональным данным, несут ответственность за разглашение конфиденциальной информации, связанной с персональными данными граждан, полученных в результате предоставления санаторно-курортных услуг - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Согласие субъекта на обработку своих персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Обществом.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Общество вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Персональные данные могут быть получены Обществом от лица, не являющегося субъектом персональных данных, при условии предоставления Обществу подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

Приложение
к Политике АО «Санаторий «Чувашия»
в отношении обработки персональных данных

Сведения о реализуемых требованиях к защите персональных данных

1. Общество обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановления Правительства Российской Федерации от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", комплекса документов в области обработки персональных данных Общества.

2. При обработке персональных данных Общество принимает необходимые правовые, организационные и технические меры или обеспечивает 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 (Таблица 1 к Приложению)

3. Обеспечение безопасности персональных данных достигается, в частности, посредством:

- определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработки моделей угроз;
- применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- проведения оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- организации учета машинных носителей персональных данных;
- обнаружения фактов несанкционированного доступа к персональным данным и принятия мер;
- восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

4. В целях обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации, в отношении каждой категории персональных данных Обществом определяются места хранения персональных данных (материальных

носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Обществом обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Обществом.

5. В целях исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при обработке персональных данных в информационных системах, Общество использует средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6. Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

7. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Классификация информационных систем персональных данных осуществляется Обществом в порядке, установленном законодательством Российской Федерации.

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. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. Обрабатываемые в информационных системах персональные данные могут быть представлены для ознакомления:

- работникам Общества, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;
- уполномоченным лицам, осуществляющим обработку персональных данных по поручению Общества на основании заключенного с ним договора;
- уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

Работники, доступ которым к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых)

обязанностей, допускаются к соответствующим персональным данным на основании утвержденного Обществом списка.

10. Запросы третьих лиц на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются в соответствующем журнале обращений.

При обнаружении нарушений порядка предоставления персональных данных Общество незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

11. В целях реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности Общества, снижения рисков нарушения информационной безопасности и управления ими Обществом назначен ответственный за организацию обработки персональных данных, который:

- осуществляет внутренний контроль за соблюдением Обществом и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводит до сведения работников Общества положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Таблица 1

Перечень мероприятий, обеспечивающих сохранность персональных данных в АО «Санаторий «Чувашия»

1. Организационные мероприятия

- Осуществление внутреннего контроля за соблюдением и его сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных
- Доведение до сведения положения законодательства РФ о персональных данных, разработанных внутренних локальных актов по вопросам обработки персональных данных, требований к защите персональных данных
- Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.
- Отслеживание изменений в процессах обработки персональных данных, установленных законодательством.
- Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними
- Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в Журнал учета с отметкой об их выдаче (приеме)

2. Физические мероприятия

- Организация хранения материальных носителей ПДн в помещениях, установка дополнительных металлических шкафов (хранилищ) и замков

3. Технические (аппаратные и программные) мероприятия

- Внедрение системы антивирусной защиты на ПК
- Внедрение системы межсетевого экранирования
- Внедрение системы защиты от НСД и криптографической защиты

4. Контролирующие мероприятия

- Контроль над соблюдением режима обработки ПДн
- Контроль над соблюдением режима защиты
- Контроль над выполнением антивирусной защиты
- Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена
- Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн
- Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн
- Контроль за обеспечением резервного копирования
- Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз
- Поддержание в актуальном состоянии нормативно-организационных документов
- Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.
- Отслеживание объемов обрабатываемых ПДн, состава обрабатываемых ПДн в различных ИСПДн, целей обработки ПДн