СОГАЗ МЕДИЦИНА	**Политика обработки и защиты персональных данных в ООО «Международный медицинский центр «СОГАЗ»**	

Приложение № 1
к Приказу от 02.11.17 № 51/А/42
«Об утверждении Политики обработки и защиты персональных данных»

1. Общие положения

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) разработана во исполнение п. 2 ст. 18.1. Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим документом ООО «Международный медицинский центр «СОГАЗ» (далее – Организация), определяющим ключевые направления деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика утверждена Приказом единоличного исполнительного органа Организации от 02.11.17 № 51/А/42.

1.3. Политика сформирована в целях реализации требований законодательства Российской Федерации в области обработки ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.4. Положения настоящей Политики распространяются, в том числе, на деятельность Организации в области обработки и защиты ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного или иного характера положения Политики не могут быть распространены на отношения, связанные с обработкой и защитой ПДн, полученных до ее утверждения.

1.5. Обработка ПДн в Организации производится в связи с осуществлением Организацией деятельности, предусмотренной ее учредительными документами, и определяемой:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств»;
- Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Также, в Организации осуществляется обработка ПДн в рамках трудовых и иных непосредственно связанных с ними отношений, при реализации которых Организация выступает в качестве работодателя (в соответствии с главой 14 Трудового кодекса Российской Федерации) и связи с реализацией Организацией своих прав и обязанностей в качестве юридического лица.

2. Термины и определения

2.1. В настоящей Политике используются следующие основные понятия.

2.1.1. **Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.1.2. **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.

2.1.3. **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 цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.1.4. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.1.5. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.1.6. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.1.7. **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.

2.1.8. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.1.9. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

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

2.1.11. **Пациент** – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

2.1.12. **Медицинская деятельность** – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

2.1.13. **Фармацевтическая деятельность** – деятельность, включающая в себя оптовую торговлю лекарственными средствами, их хранение, перевозку и (или) розничную торговлю лекарственными препаратами, их отпуск, хранение, перевозку, изготовление лекарственных препаратов.

2.1.14. **Медицинская помощь** – комплекс мероприятий, направленных на поддержание и (или) восстановление здоровья и включающих в себя предоставление медицинских услуг.

2.2. Термины и определения, не определенные настоящей Политикой, трактуются в соответствии с законодательством Российской Федерации.

3. Цели и основания обработки ПДн

3.1. Сбор и обработка ПДн в Организации осуществляется в следующих целях.

- Осуществление деятельности в области здравоохранения, обеспечения оказания медицинской помощи, фармацевтической и иных видов деятельности, предусмотренных учредительными документами Организации.
- Осуществление трудовых отношений.
- Осуществление гражданско-правовых отношений.

3.2. Обработка в Организации ПДн осуществляется на следующих правовых основаниях.

- Федеральные законы Российской Федерации и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Организации, предусмотренной учредительными документами, включая: Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», Федеральный закон от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правила предоставления медицинскими организациями платных медицинских услуг, утвержденные Постановлением Правительства Российской Федерации от 04 октября 2012 г. № 1006.
- Учредительные документы Организации.
- Договоры, заключаемые между Организацией и субъектом ПДн.
- Согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям Организации).

3.3. В Организации, в рамках достижения установленных целей обработки ПДн, осуществляется обработка ПДн следующих субъектов.

- Пациенты (клиенты) Организации и контрагенты (физические лица), а также их представители/работники (ПДн, полученные при осуществлении деятельности в области здравоохранения, обеспечении оказания медицинской помощи, осуществлении фармацевтической и иных видов деятельности, предусмотренных учредительными документами Организации, в том числе, полученные при осуществлении гражданско-правовых отношений).
- Работники Организации, бывшие работники, а также родственники работников (ПДн, полученные в рамках трудовых отношений в соответствии с законодательством Российской Федерации).

- Кандидаты на замещение вакантных должностей (ПДн, предоставленные для принятия решения о соответствии кандидата установленным законодательством Российской Федерации и Организацией требованиям).
- Иные лица, предоставившие Организации свои ПДн для обработки в случаях, предусмотренных законодательством Российской Федерации, предоставившие Организации согласие на обработку своих ПДн, либо сделавшие свои ПДн общедоступными, в случаях и в целях, не противоречащих законодательству Российской Федерации.

4. Порядок и условия обработки ПДн

4.1. Обработка ПДн в Организации осуществляется на законной и справедливой основе и ограничивается достижением целей, установленных требованиями законодательства Российской Федерации и настоящей Политики. Обработка ПДн, несовместимая с целями сбора ПДн, не допускается.

4.2. Обработка персональных данных в Организации осуществляется:

- с согласия субъекта ПДн на обработку его ПДн;
- в случаях, когда обработка ПДн необходима для осуществления и выполнения установленных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.

4.3. Обработке в Организации подлежат только ПДн, которые отвечают установленным целям их обработки. В Организации обеспечивается соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.4. Обработка ПДн в Организации может осуществляться как с использованием средств автоматизации, так и без использования таких средств путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения, в том числе, с передачей по информационно-коммуникационной сети Интернет.

4.5. В процессе обработки ПДн, в порядке, установленном законодательством Российской Федерации, может осуществляться трансграничная передача ПДн на территорию иностранных государств.

4.6. При обработке ПДн Организацией должна обеспечиваться их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки. Организация обеспечивает принятие мер по удалению или уточнению неполных или неточных данных.

4.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

4.8. Обрабатываемые Организацией ПДн подлежат уничтожению либо обезличиванию при достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.9. Организация обеспечивает конфиденциальность ПДн при их обработке, не раскрывает третьим лицам и не распространяет ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом. Организация вправе передавать ПДн по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора; в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5. Обеспечение безопасности ПДн при их обработке

5.1. В Организации, в целях обеспечения безопасности ПДн, обеспечивается применение мер, предусмотренных Федеральным законом от 27.07.2006 «О персональных данных» № 152-ФЗ.

5.1.1. Организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, установленных федеральными законами и нормативными Российской Федерации, регулирующими вопросы обработки ПДн, если иное не предусмотрено федеральными законами.

5.1.2. К мерам, применяемым в Организации в целях обеспечения безопасности обработки ПДн, относятся, в том числе:

- назначение лица, ответственного за организацию обработки ПДн;
- применение правовых, организационных и технических мер по обеспечению защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- ознакомление работников Организации, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите ПДн, а также документами Организации, регулирующими вопросы обработки ПДн;
- осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн требованиям законодательства и нормативных правовых актов в области защиты ПДн, настоящей Политики, внутренних документов Организации, регулирующих вопросы обеспечения безопасности ПДн при их обработке.

5.1.3. Состав и перечень мер, используемых в Организации в целях обеспечения безопасности обработки ПДн, а также порядок их применения устанавливаются внутренними документами Организации.

5.2. В Организации обеспечивается безопасность ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации, включая, в том числе, следующие меры.

5.2.1. При обработке ПДн без использования средств автоматизации: обеспечивается применение мер, исключающих несанкционированный доступ к ПДн; определен

перечень лиц, осуществляющих обработку ПДн; определены места хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях.

5.2.2. При обработке ПДн с использованием средств автоматизации на основе модели угроз разработана система защиты ПДн, направленная на нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн.

5.2.3. Определен перечень лиц, допущенных к обработке ПДн в ИСПДн.

5.2.4. Лица, допущенные к эксплуатации применяемых при обеспечении безопасности ПДН средств защиты информации, обучены правилам работы с ними.

5.2.5. Помещения, в которых размещены ИСПДн и носители ПДн, оборудованы необходимыми средствами защиты от проникновения и пребывания в них посторонних лиц.

6. Права субъекта ПДн

6.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- правовые основания и цели обработки ПДн;
- цели и применяемые способы обработки ПДн;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

6.2. Субъект ПДн вправе требовать уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн субъекта являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством меры по защите своих прав.

6.3. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и устанавливается внутренними документами Организации.

6.4. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии федеральными законами, в том числе, если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

7. Обязанности Организации

7.1. При сборе ПДн Организация обязана предоставить субъекту ПДн по его просьбе информацию, обозначенную в п. 6.1. настоящей Политики.

7.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Организация обязана разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

7.3. Если ПДн получены не от субъекта ПДн, Организация, за исключением случаев, предусмотренных федеральными законами, до начала обработки таких ПДн, обязана предоставить субъекту ПДн информацию об источнике получения ПДн, целях и правовых основаниях обработки ПДн, предполагаемых пользователях ПДн и иные сведения в отношении обработки ПДн субъекта, предусмотренные федеральным законом.

7.4. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», Организация обязана обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных федеральными законами.

7.5. Организация, в течение срока и в порядке, установленными федеральными законами, обязана обеспечить прекращение обработки ПДн и их уничтожение в случае выявления неправомерной обработки ПДн, при достижении цели обработки ПДн, в случае отзыва субъектом ПДн согласия на обработку ПДн (за исключением случаев, предусмотренных федеральными законами).

8. Заключительные Положения

8.1. Контроль реализации положений настоящей Политики осуществляется лицом, ответственным за организацию обработки ПДн в Организации.

8.2. Организация, а также работники Организации несут установленную законодательством Российской Федерации ответственность за нарушение требований законодательства в области обработки ПДн.

8.3. Официальная действующая редакция Политики хранится по месту нахождения Организации по адресу: 191186, Санкт-Петербург, Чебоксарский переулок, дом 1/6, лит. «А». Электронная версия действующей редакции Политики доступна неограниченному кругу лиц на официальном сайте Организации по адресу: http://www.sogaz-clinic.ru.

8.4. Организация может вносить изменения в настоящую Политику, в том числе, в случае внесения изменений в законодательство Российской Федерации о персональных данных. Новая редакция Политики вступает в силу с даты ее размещения на официальном сайте Организации, если иное не предусмотрено новой редакцией Политики.

8.5. По вопросам, связанным с обработкой и защитой ПДн в Организации, следует обращаться по месту нахождения Организации.