



Политика обработки и защиты персональных данных

1. Общие положения

1.1. Настоящее Положение в отношении политики обработки и защиты персональных данных (далее - Положение) составлено в соответствии с п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и является основополагающим внутренним регулятивным документом ООО «Медицинский центр Покровский», определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является ООО «Медицинский центр Покровский».

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в ООО «Медицинский центр Покровский», в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положение распространяется на отношения по обработке и защите ПДн, полученных ООО «Медицинский центр Покровский» как до, так и после утверждения Положения, за исключением случаев, когда по причинам правового, организационного и иного характера Положения не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в ООО «Медицинский центр Покровский» осуществляется в связи с выполнением функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в ООО «Медицинский центр Покровский» осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых ООО «Медицинский центр Покровский» выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией своих прав и обязанностей как юридического лица.

1.5. ООО «Медицинский центр Покровский» имеет право вносить изменения в настоящее Положение.

2. Термины и принятые сокращения

- 2.1. Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2.2. 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;
- 2.3. 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;
- 2.4. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 2.5. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 2.6. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 2.7. Уничтожение персональных данных- действия, в результате которых становится невозможным восстановить содержание персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- 2.8. Обезличивание персональных данных- действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 2.9. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- 2.10. Пациент - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;
- 2.11. 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.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в ООО «Медицинский центр Покровский» является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн ООО «Медицинский центр Покровский» руководствуется следующими принципами:

- *законность*: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области

обработки и защиты ПДн;

- *системность*: обработка ПДн в ООО «Медицинский центр Покровский» осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

- *комплексность*: защита ПДн строится с использованием функциональных возможностей информационных технологий и других имеющихся систем и средств защиты;

- *непрерывность*: защита ПДн обеспечивается на всех этапах их обработки;

- *своевременность*: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

- *преемственность и непрерывность совершенствования*: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

- *персональная ответственность*: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- *минимизация прав доступа*: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

- *гибкость*: обеспечение выполнения функций защиты ПДн при изменении также объема и состава обрабатываемых ПДн;

- *специализация и профессионализм*: реализация мер по обеспечению безопасности ПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;

- *эффективность процедур отбора кадров*: кадровая политика ООО «Медицинский центр Покровский» предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

- *наблюдаемость и прозрачность*: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

- *непрерывность контроля и оценки*: устанавливаются процедуры постоянного контроля осуществления обработки ПДн, а результаты контроля регулярно анализируются.

3.3. В ООО «Медицинский центр Покровский» не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся ООО «Медицинский центр Покровский» ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. ООО «Медицинский центр Покровский» принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4. Обработка персональных данных

4.1. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с

Федеральными законами от 21.11.2011 № 323-03 «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4.10.2012 № 1006;

- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2. Категории субъектов персональных данных

В ООО «Медицинский центр Покровский» обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

4.3. ПДн, обрабатываемые ООО «Медицинский центр Покровский»:

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

4.4. Обработка персональных данных ведется:

- с использованием средств автоматизации.
- без использования средств автоматизации.

4.5. Получение ПДн.

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

4.5.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.5.3. Документы, содержащие ПДн создаются путем:

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

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Оператором, определяется в соответствии с законодательством и определяется внутренними регулятивными документами ООО «Медицинский центр Покровский».

4.6. Обработка ПДн.

4.6.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

4.6.2. Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов ООО «Медицинский центр Покровский».

4.6.3. Допущенные к обработке ПДн работники под роспись знакомятся с документами ООО «Медицинского центра Покровский», устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

4.7. Обработка ПДн пациентов в ООО «Медицинского центра Покровский».

4.7.1. Пациент может оставить в ООО «Медицинский центр Покровский» три вида персональных данных:

- персональные данные - адрес постоянного проживания, контактный телефон, паспортные данные;

- специальные данные о здоровье (субъекта персональных данных - пациента) - вся информация, касающаяся здоровья, предоставленного лечения, включая информацию о самом факте обращения в медицинскую организацию, - это данные, которые заносятся в медицинскую карту;

- биометрические данные (субъекта персональных данных - пациента) - любая информация о физиологических и биологических особенностях человека, на основании которых можно установить его личность (рентгеновские снимки, фотографии и пр.).

4.7.2. При первом визите в организацию ООО «Медицинский центр Покровский» пациенту предлагается заполнить бланк информированного добровольного согласия на обработку персональных данных. При последующих посещениях ООО «Медицинского центра Покровский» информация о персональных данных (или их изменении) может уточняться работниками регистратуры.

4.7.3. Полученные сведения накапливаются в ООО «Медицинский центр Покровский», хранятся и используются медицинским персоналом при оказании медицинских услуг.

4.7.4. Отказ пациента от дачи письменного согласия на обработку его персональных данных не является основанием для неоказания ему медицинских услуг в ООО «Мейли».

4.8. Хранение ПДн.

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

4.8.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

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

4.8.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных источниках.

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

4.9. Уничтожение ПДн.

4.9.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в

бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

4.9.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

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

4.10. Передача ПДн.

4.10.1. ООО «Медицинский центр Покровский» передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.10.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

- Пенсионный фонд Российской Федерации для учета (на законных основаниях);
- Налоговые органы Российской Федерации (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические фирмы, работающие в рамках законодательства Российской Федерации, при неисполнении обязательств по договору займа (с согласия субъекта).

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов ООО «Медицинский центр Покровский» создана система защиты персональных данных.

5.2. Основными мерами защиты ПДн, используемыми ООО «Медицинский центр Покровский», являются:

5.2.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

5.2.2. Определение актуальных угроз безопасности ПДн при их обработке и разработка мер и мероприятий по защите ПДн;

5.2.3. Разработка политики в отношении обработки персональных данных;

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

5.2.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;

5.2.6. Установление индивидуальных паролей доступа сотрудников для работы с ПДн в электронном виде в соответствии с их производственными обязанностями;

5.2.7. Соблюдение условий, обеспечивающих сохранность ПДн и исключющие несанкционированный к ним доступ, оценка эффективности принимаемых и

реализованных мер по обеспечению безопасности ПДн;

5.2.8. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.2.9. Обучение работников ООО «Медицинский центр Покровский» непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику ООО «Медицинский центр Покровский» в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

5.2.10. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПДн и обязанности Оператора

6.1. Основные права субъекта ПДн

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором 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 № 152-ФЗ от 27.07.2006 «О персональных данных»;
- 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 настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе отозвать свое согласие на обработку ПДн путем уведомления об этом Оператора в письменном виде в установленном порядке.

Субъект ПДн вправе требовать от оператора 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.

6.2. Обязанности Оператора

Оператор ПДн обязан:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к

документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;

- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.