утверждено
протоколом № 21 от 25.12.15г.
общего собрания участников
ООО «Британская Медицинская Компания»

Положение
об обработке и защите персональных данных
в Обществе с ограниченной ответственностью «Британская Медицинская Компания»

1. Общие положения

1.1. Настоящее Положение в отношении обработки персональных данных (далее - Положение) составлено в соответствии с п. 2 ст. 18.1 Федерального закона Российской Федерации «О персональных данных» № 152-ФЗ от 27 июля 2006 года а также иных нормативно-правовых актов Российской Федерации в области защиты и обработки персональных данных (далее ПД) и является основополагающим внутренним регулятивным документом ООО «Британская Медицинская Компания» (далее по тексту - Оператор, центр), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных.
1.2. Положение разработано в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД Оператором, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.
1.3. Положение распространяется на отношения по обработке и защите ПД, полученных Оператором как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до ее утверждения.
1.4. Обработка ПД осуществляется в связи с выполнением Оператором функций, предусмотренных ее учредительными документами, и определяемых:
- Федеральным законом Российской Федерации от 21 ноября 2011г. № 323-ФЗ «Об основах охраны здоровья граждан в РФ»;
- Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки ПД, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных;
- иными нормативными правовыми актами Российской Федерации.
1.5. Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями законодательства РФ.
1.6. Оператор имеет право вносить изменения в настоящее Положение. При внесении изменений в заголовке Положения указывается дата последнего обновления редакции. Новая редакция Положения вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Положения.

1.7. Деиствующая редакция хранится в месте нахождения Оператора по адресу: 236010, город Калининград, проспект Мира, 136, кабинет 7; электронная версия положения на сайте Оператора по адресу: http:// bmc-dial.ru

2. Термины и принятые сокращения

Персональные данные (ПД) - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). В состав обрабатываемых Оператором персональных данных пациентов может входить, в том числе: Ф.И.О пациента, его пол; дата и место рождения; гражданство; данные документа, удостоверяющего личность пациента; место жительства и/или место регистрации; место работы/учебы; контактный телефон и адрес электронной почты; полис ОМС; СНИЛС; ИНН; анамнез и диагноз; сведения об организации, оказавшей медицинскую помощь и вид оказанной медицинской помощи; условия оказания медицинской помощи; сроки оказания медицинской помощи; объём оказанной медицинской помощи; результат обращения за медицинской помощью; серия и номер выданного листка нетрудоспособности (при наличии); сведения об оказанных медицинских услугах; примененные стандарты медицинской помощи; сведения об медицинском работнике или работниках, оказавших медицинскую услугу; другая информация, необходимая для выполнения обязательств Оператором в соответствии с законодательством РФ.

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;

Оператор — государственный/муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПД, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В контексте данного положения Оператором является ООО «Британская Медицинская Компания»;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

3. Принципы обеспечения безопасности персональных данных

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

3.2. Для обеспечения безопасности ПД Организация руководствуется следующими принципами:

- законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;
- системность: обработка ПД в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;
- комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки в Организации с учетом выявления новых средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПД;
- минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых данных;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляется Работниками, имеющими необходимые квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПД уничтожаются или обезличиваются.

3.4. При обработке ПД обеспечиваются их точность, достаточность, при необходимости - и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПД.

4. Обработка персональных данных

4.1. Получение ПД.

4.1.1. Все ПД следует получать от самого субъекта лично или от его законного представителя. Если ПД субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

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

4.1.3. Документы, содержащие ПД создаются/получаются путем:

- получения данных при их предоставлении субъектом (паспорт, свидетельство ИНН, страховой медицинский полис и др.);
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение и др.);
- внесения в информационные системы Оператора.

Порядок доступа субъекта ПД к его ПД, обрабатываемым Организацией, определяется в соответствии с законодательством и внутренними регулятивными документами Организации.

4.2. Обработка ПД

4.2.1. 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).

Доступ Работников к обрабатываемым ПД осуществляется в соответствии с их должностными инструкциями и требованиями внутренних документов Организации. Допущенные к обработке ПД Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПД.

4.2.2. Цели обработки персональных данных:

- Обеспечение Оператором оказания медицинской помощи пациентам, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ; «Об обязательном медицинском страховании граждан в Российской Федерации» от 29 ноября 2010 года № 326-ФЗ;
- Осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных.

У оператора обрабатываются ПД следующих субъектов ПД :

- физические лица, состоящие с оператором в гражданско-правовых отношениях
- физические лица, обратившиеся к оператору за медицинской помощью.

4.2.4. ПД, обрабатываемые Оператором:

- Данные полученные при осуществлении гражданско-правовых отношений.
- Данные полученные при оказании медицинской помощи

4.2.5. Обработка персональных данных ведется:

- С использованием средств автоматизации
- Без использования средств автоматизации

4.3. Хранение ПД

4.3.1. ПД Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
4.3.2. ПД, зафиксированные на бумажных носителях хранятся в обособленных подразделениях Оператора в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.
4.3.3. ПД Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).
4.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.
4.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, 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.
4.4. Уничтожение ПД
3.4.1. Уничтожение документов (носителей), содержащих ПД производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.
4.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.
4.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.
4.5. Передача ПД
4.5.1. Оператор передает ПД третьим лицам в следующих случаях:
- Субъект выразил свое согласие на такие действия;
- Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются ПД.
Третьи лица, которым передаются ПД:
- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (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);
- Органы дознания, следствия, прокуратуры и суда в случаях, установленных законодательством.

5. Защита персональных данных

5.1. Основными мерами защиты ПД, используемыми Оператором, являются:
5.1.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Оператором (Обществом и его обособленными подразделениями) и его работниками требований к защите ПД;
5.1.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;
5.1.3. Разработка политики в отношении обработки персональных данных;
5.1.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД;
5.1.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
5.1.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
5.1.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
5.1.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.1.9. Соолюдаются условия, ооеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ;
5.1.10. Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
5.1.11. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
5.1.12. Обучение работников Оператора непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
5.1.13. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПД и обязанности оператора

6.1. Основные права субъекта ПД
Субъект имеет право на доступ к его персональным данным и следующим сведениям:
- подтверждение факта обработки ПД оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с оператором или на основании федерального закона;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;
- обращения к оператору и направлению ему запросов;
- обжалование действий или бездействия оператора.
Субъект ПД 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 обязан:
- при сборе ПД предоставить информацию об обработке ПД;
- в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения Субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.